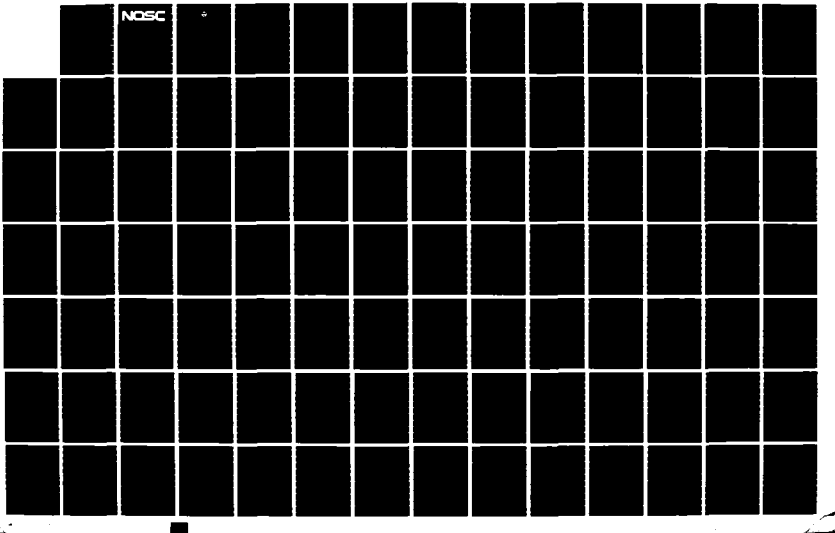
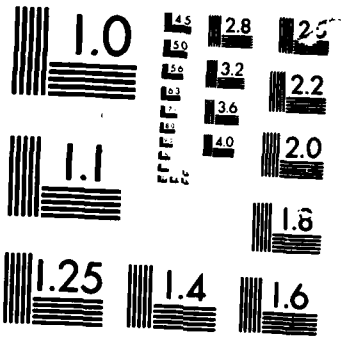
AD-A169 008 FAULT-TOLERANT SYSTEMS TECHNOLOGY PROGRAM PLAN: A CONCENTRATED PRIORITIZE..(U) NAVAL OCEAN SYSTEMS CENTER SAN DIEGO CA W J DEJKA 01 AUG 77 NOSC/TD-131 1/2

UNCLASSIFIED F/G 5/1 NL





MICROCOP CHART

(2)

NOSC

NOSC / TD 131

AD-A169 008

NOSC / TD 131

Technical Document 131

FAULT-TOLERANT SYSTEMS TECHNOLOGY PROGRAM PLAN

A concentrated, prioritized, and phased R&D program is proposed for the development of the technology

WJ Dejka

1 August 1977

DTIC FILE COPY

ELECTE
JUN 30 1986
S
E

Approved for public release; distribution is unlimited

NAVAL OCEAN SYSTEMS CENTER
SAN DIEGO, CALIFORNIA 92152

86 6 30 074

NAVAL OCEAN SYSTEMS CENTER, SAN DIEGO, CA 92152

AN ACTIVITY OF THE NAVAL MATERIAL COMMAND

RR GAVAZZI, CAPT USN
Commander

HL BLOOD
Technical Director

ADMINISTRATIVE INFORMATION

This project was funded under Air Force task element 62204F – AF and Navy element 62762N (R138000). Dr Charles Brodnax of the Air Force Avionics Laboratory was the technical manager. The efforts of many researchers in fault tolerance have contributed to the content of this plan and their help is appreciated.

Released under authority of
LZ Maudlin, Head
Computer Sciences and Simulation Department

FAULT-TOLERANT SYSTEMS WORKSHOP ROSTER

Mr Joel Trimble
Office of Naval Research

Dr C Brodnax
Major Bush
AFAL
Wright-Patterson Air Force Base

Dr William Saunders
Director Electronics
Department of the Army
US Army Research Office

Dr Liba Svobodova
Dave Jensen
Massachusetts Institute of Technology

Dr Dan Siewiorek
Carnegie-Mellon University
Computer Science Department

Mr Larry Jack
Honeywell Systems and Research

Mr Cay Weitzman
TRW

Dr Ralph Martinez
Code 923
NOSC

Dr FG Gray
VPI State University
Department of EE

Dr Don Calhoun
Hughes Aircraft

Dr EJ McCluskey
Digital Systems Laboratory
Stanford University

Mr Buddy Dean
Texas Instruments

Mr Jack Goldberg
SRI

Dr AA Avizienis
University of California at Los Angeles

Al Hopkins
Draper Laboratories

John Weber
ASD - WPAFB

Dr Dave Goodman
DAVEX ENG

Chuck Arnold
NUSC, New London

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NOSC Technical Document 131 (TD 131)	2. GOVT ACCESSION NO. AD-A169008	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* FAULT-TOLERANT SYSTEMS TECHNOLOGY PROGRAM PLAN (A concentrated, prioritized, and phased R&D program is proposed for the development of the technology)		5. TYPE OF REPORT & PERIOD COVERED 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR*(s)* WJ Dejka		8. CONTRACT OR GRANT NUMBER*(s)*
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Ocean Systems Center San Diego, California 92152		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 62760N, F53537, XF53537001 (NOSC R138)
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Material Command Test & Monitoring Systems Office Washington, DC 20360		12. REPORT DATE 1 August 1977 13. NUMBER OF PAGES 114
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution is unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Automatic test equipment
Command control
Communications
Performance monitoring

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This document attributes the relative neglect of fault tolerance in system specification to a number of factors including inadequacy of specifications, the undeveloped state of applicable techniques, and fragmentation of effort among disciplines. It recommends the development of the technology and routine application to system acquisition. It describes major projects within the discipline and summarizes the state of the art.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-LF-014-6601

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

EXECUTIVE SUMMARY

PROGRAM PLAN FOR DEVELOPMENT OF FAULT-TOLERANT SYSTEM TECHNOLOGY

FAULTS AND TOLERANCE

A fault is an abnormal condition the appearance of which may force a system into an error state leading to partial or complete failure to execute its required function. Tolerance is that property which allows the system to perform in the expected way despite the appearance of explicitly specified classes of potentially disabling faults.

VALUE TO THE SYSTEM

Fault tolerance is related to both reliability and maintainability. One of the projects within this program plan, in fact, is concerned precisely with defining reliability and maintainability to take into consideration degrees of tolerance and other factors not presently considered so that fault tolerance technology may be more effectively applied.

With reliability and maintainability fault tolerance significantly affects system effectiveness, logistic supportability, and life-cycle cost.

Unavailability at a time of critical need could result in loss of men, material and tactical advantage. Effectiveness is totally dependent upon availability and availability is directly proportional to the fault tolerance of the system.

Supportability requires a match between system maintenance needs and available maintenance resources. Continuing growth of system complexity is tolerable only if the accompanying maintenance requirements are prevented somehow from rising through the ceiling. Built-in test and other fault tolerance techniques must be employed to keep this from happening. With BIT, one internal failure can be detected and corrected at a reasonable expenditure of energy and time before another follows and the system is out of combat altogether.

System life-cycle costs range from 3 to 20 times procurement costs, and maintenance costs make up a large slice of the pie. Test equipment, training, and documentation contribute heavily to maintenance costs, but the measure of each of them can be held down through fault tolerance.

So fault tolerance contributes to military systems in the areas of effectiveness, supportability, and life-cycle cost. What value can be put upon it? This must be measured against the importance of the system to the mission. Fault tolerance may be an unnecessary refinement in one application, merely desirable in a second, and essential in the third.

In a mission-critical system such as V/STOL (vertical/short take off and landing aircraft), for example, it must be considered essential on the basis of the following and other contributions:

It minimizes risks to users and equipment associated with component and device failure.

It eliminates unacceptable maintenance downtime in real-time environments.

It allows systems to be used in environments to which access is restricted.

It opens the possibility of lower total life-cycle costs and of lower initial costs for a given reliability goal.

It provides psychological support to system users.

ROADBLOCKS

A program for the development and implementation of a technology promising all these advantages should not be difficult to promote. It would be well, nevertheless, to look closely at the state of the art today before we plot our route to the mature and usable technology of the future. We find it is characterized by a number of lacks, by fragmentation, by inertia, and by resistance.

LACK OF CONTINUITY. Some fault tolerance techniques were developed for first-generation computers but were discarded because the second-generation computer demonstrated much higher reliability in semiconductor and magnetic-core components. In addition, many problem solutions were not openly documented, causing much reinvention of techniques. Also, many errors were repeated with subsequent loss of confidence in those techniques.

LACK OF COST/BENEFIT MEASURES. To date there are no general methods for a convenient quantitative assessment of the benefits of fault tolerance in terms of life-cycle cost reduction. The initial extra cost due to the use of redundancy techniques is more directly evident and tends to bias in favor of systems without fault tolerance a large class of users who do not have an absolute requirement.

LACK OF SPECIFICATIONS AND ACCEPTANCE TESTS. The user community at large does not have adequate knowledge of the properties and limitations of fault tolerance. As a consequence, specifications for reliability are insufficiently precise and virtually unverifiable in advance of system use. For example, reliability requirements for a given time interval do not specify classes of faults and do not define what constitutes acceptable recovery.

FRAGMENTATION OF EFFORT. Program efforts to increase reliability of systems originate within several disciplines of engineering theory and practice. These include system architecture, software engineering, testing and design verification, design of data base management systems, computer networks and communication systems, component and packaging engineering, and field operation and maintenance. Although they have a common goal, these efforts have remained largely disjointed. A lack of common viewpoint and systematic communication is evident. There is also a gap between the results of theoretical investigations and practical engineering solutions to fault tolerance problems.

INERTIA IN THE DESIGN PROCESS. Introduction of fault tolerance in system design requires an early commitment and a significant departure from the traditional evolutionary design of system or subsystem "product line" in which compatibility of software is usually a dominant factor. While the number of fault tolerance techniques at hand to serve as maintenance aids has been increasing, none of the major manufacturers have announced a fully fault-tolerant line of computers or subsystems. The only fault-tolerant systems actually delivered have been custom made to special requirements.

PROGRAM PLAN – THREE OBJECTIVES AND 32 PROJECTS

The Naval Ocean Systems Center (NOSC) with Air Force sponsorship has developed a Fault Tolerance Program Plan which represents a systematic assault on the roadblocks described above. It has three prime objectives and is structured in 32 individual projects. The objectives and the projects associated with them are listed below. Several projects apply to two objectives, and one applies to three. Top-priority projects are asterisked.

1. Clarify operational requirements and relate them to system specifications.

   Fault Tolerance Requirements Definition and Interpretation*

   Mission Availability Analysis Methods*

   Project DAIS Fault Tolerance Evaluation*

   Relation of Requirements to Specification*

   Command Control Fault Tolerance*

   Standards and Fault Tolerance*

   Self-Diagnosing Design Techniques*

   Design/Development Tools (Methodology)*

   TECHEVAL-OPEVAL Techniques*

   Fault Tolerance Design Handbook

   Specification for Redundancy Management

   Architectures for Availability Requirements

2. Establish alternate system design method for balancing operational capabilities against life-cycle costs.

   Self-Diagnosing Design Techniques*

   Design/Development Tools (Methodology)*

   Acceptance Testing*

   Establishment of Redundancy Limits/Tradeoffs

   Failure-Fault Prediction Technology

   Recovery Techniques

   Transient Faults

   Identification of Failure Modes

   Fault-Tolerant Software

   Analog Functional Redundancy

   Estimation of Confidence Limits Testing Large Logic Networks

   Redundant Microcomputers

   Loosely Coupled Fault-Tolerant Computer Networks

   Fault Tolerance Masking Hazards

   Fault Tolerance Design Handbook

   Reliability/Fault Tolerance Analysis and Design Tools

QUALITY INSPECTED 3

Accession
NTIS
DTIC
By
Dist
A-1

3. Develop understanding of system engineering relationships between reliability, fault tolerance, repairability, and logistics support.

Fault Tolerance Life-Cycle Cost Impacts – Maintenance Model*

Theory of Testing – Taxonomy*

Reliability – Measure of Testability Concept*

High-Order Language Constructs for Fault-Tolerant Systems*

Functional Test Design Theory*

Fault Tolerance – Validation and Verification*

Acceptance Testing*

Standards and Fault Tolerance*

TECHEVAL-OPEVAL Techniques*

Communication Protocol for Fault Tolerance

Reliability/Fault Tolerance Analysis and Design Tools

Alternate System Design Evaluation

Fault Tolerance Masking Hazards

Fault Tolerance Design Handbook

You will have noticed that the Fault Tolerance Design Handbook is the project common to all three objectives.

IMPLEMENTATION STRATEGY

Development of the fault tolerance technology by the military must be in consonance with the efforts of other governmental, industrial, and university organizations. It must exploit the results of related research supported by National Science Foundation, National Aeronautics and Space Agency, and other organizations.

Cost and technical risk will not allow development of fault tolerance technology for a single specific system. The technology must be applicable to all systems. Basic ideas must be funded first. Initial targets for application must be as broad as electronics/avionics, communications, surveillance, and command control. Later effort can be funneled into such specific fields as computer netting, human error in systems, data base fault tolerance, fault-tolerant hardware, and fault/failure prediction.

The military must sponsor technology transfer between DoD and civilian communities. Application-oriented workshops are suggested as one effective medium. It is also strongly recommended that the military supply the needed fault tolerance literature – developing, maintaining, and distributing a series of publications that reflect the baseline of the technology.

CONTENTS

ILLUSTRATIONS

TABLES

1.0 The Fault Tolerance Problem

1.1 Purpose of the plan. Military goals and strategies strongly emphasize increased system availability, simplified maintenance, and reduced life-cycle costs. Yet, the technical areas of reliability, fault tolerance, and maintainability (which are paramount to mission success in tactical systems) suffer from several critical problems. Solutions to these problems are the objective of this research and development program plan. The basic objectives of the program plan are:

a. To clarify operational requirements and to relate them to statement of system specifications

b. To establish a method for evaluating alternate system designs that balance operational capability against life-cycle costs, especially for degraded modes of operation

c. To develop understanding of system engineering relationships between reliability, fault tolerance, repairability, and support

Some specific problems related to the rapid advance in technology and the increasing complexity of systems are:

a. Disparity in evolution of fault-tolerant design and LSI technology

b. Lack of system reliability and performance estimation tools for risk analysis, design, and system verification

c. Lack of awareness on the part of designers of the various techniques for designing fault-tolerant systems

d. Lack of evaluation methods for proving the effectiveness of fault tolerance

Modern design of a system of the future requires the understanding of systems operation, reliability design, fault tolerance partitioning, maintenance design (including the operation and design of equally complex test equipment), and other aspects of the overall design process. This program plan is based on addressing these needs from an integrated viewpoint, beginning with operational requirements and ending with final system acceptance testing and evaluation. This plan is written to achieve the development of fault-tolerant systems technology through a concentrated, prioritized, and phased program.

1.2 Definition of fault tolerance. A fault is an abnormal condition that appears during the operation of a system. Its appearance may or may not cause a departure from the expected behavior and force the system into an undesirable (error) state or sequence of error status. The arrival at an error state, in turn, leads to a partial or complete failure of the system to execute the required function unless provisions exist to cause a return to the expected behavior. Causes of faults are either adverse physical phenomena that can be a temporary or a permanent failure, an external interface, or human error. Because of their disruptive effect on system operation, the avoidance and/or tolerance of faults are system problems involving and related to the design, analysis, management, maintenance, and use of systems.

Fault tolerance is that property of a system that allows the system to perform in an expected way regardless of the appearance of certain (explicitly specified) classes of faults that would otherwise force the system into an error state.

Fault tolerance is related to both reliability and maintainability. The ease and rapidity with which a failed subsystem or equipment can be restored to operational status after a failure directly affects the fault tolerance of the system. For example, if there is single

redundancy of a particular subsystem and there is one failure, the system then becomes fault-intolerant until the repair is completed. This fault intolerance period is a characteristic of design and installation which is expressed as a probability that an item will be retained in, or restored to, a specified condition within a given period of time when prescribed recovery techniques are performed.

This fault intolerance measure, shown in figure 1, can be expressed either as a measure of the time (T) required to recover from a given percentage of all failures, or as a probability (P) of restoring the system to operational status within a period of time following a fault or failure.

1.3 Fault tolerance-maintainability relationship. There is an important relationship between fault tolerance and system maintainability. Both deal with the properties of the entire system under the appearance of classes of faults and/or failures. Both areas are concerned with detection and location of faults/failures. After detection and location, fault tolerance is concerned with recovery procedures, while maintainability is concerned with repairability.

In fact, the relationship is so close that fault tolerance should necessarily be considered a part of maintainability or vice versa. Additionally, this view simplifies and strengthens the designer's concept of fault tolerance and ultimately will produce systems that are more effective. This is true even for systems such as satellite electronics which cannot conveniently be repaired; however, the functional partitioning and structure of hardware are improved by mechanical design. Hierarchical design into functional and mechanical modules and components is critical to the entire design process.

It should be noted that fault tolerance and maintainability are not necessarily always correlated in a positive sense. Redundancy for fault tolerance can have the effect of masking faults and of compounding the fault-detection problem. Care must be taken during design to ensure that faults are not masked from the maintenance man, else overall system reliability will suffer.

1.4 Importance of fault tolerance. The basic value of a system is determined by three fundamental factors: system effectiveness, logistic supportability, and life-cycle costs. All three are dependent on the reliability, fault tolerance, and maintainability characteristics of the system, and all should be an important consideration in planning acquisition of a new system.

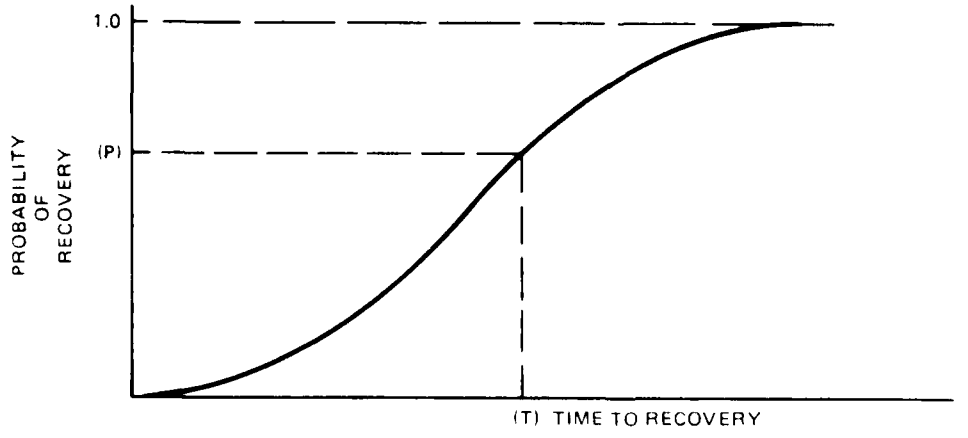


Figure 1 Fault intolerance measurement.

a. System effectiveness. Reliability, performance capability, and availability are primary measures of system effectiveness. Availability and its several deviations (eg, turnaround time, operational availability, ready rate, etc) are directly proportional to the fault-tolerant characteristics of the system. A fault-tolerant system is more often operable at the instant it is needed. Also, it can be quickly maintainable because it has built-in/designed-in fault detection and location capability. A fault-tolerant system is an important consideration when it is recognized that unavailability of a system at a time of critical need could result in loss of men, material, and tactical advantage.

Unless special care is taken in fault-tolerant system design, built-in redundancy can mask faults during the early portion of system life. As redundancy is exhausted, the probability of failure is increased. It is critical that fault-tolerant design include indication of faults as they occur so that repairs can be made immediately.

b. Logistic supportability. Maintenance requires skilled personnel in quantities and skill levels commensurate with the complexity of the system. However, the balance of that relationship cannot be maintained. System complexity has increased to the point at which the skill level and quantities of maintenance personnel for system maintenance cannot be achieved. A system should be designed to be fault-tolerant to ensure it will continue to operate even though there has been an internal failure. Built-in-test should be designed so that the system can be quickly restored to service by available maintenance and operating personnel before another failure occurs and causes a total failure of the system. This is particularly important since the typical technician may be 20 years old with approximately 40 weeks of formal schooling and usually with no more than 2 years of experience.

c. Life-cycle costs. Critical to life-cycle costs of any system are the labor-intensive operations requiring training and expensive equipment. Maintenance is a costly operation and can be significantly reduced by fault tolerance and maintenance design. Significant savings in system costs involving test equipment, training, and documentation represent only a portion of the savings in maintenance time and down-time that can be achieved. Often system life-cycle costs range from 3 to 20 times their original procurement cost.

The initial procurement cost must be a constraint on system design. There is always a budget available for systems purchase; but if the improvement in life-cycle cost causes the procurement cost to significantly increase, the improvement may not be affordable simply because we do not have the funds available for that initial purchase.

1.5 Potential of fault tolerance. The acceptance and general use of full fault tolerance (without manual intervention) can meet several military requirements:

a. Minimize the risks associated with component and device failures, in which the failures either endanger human lives or threaten catastrophic loss to the users. Examples are systems for air traffic control, guidance and control of vehicles and equipment, and other surveillance, weapons control, and navigation sensors.

b. Provide reliable (fault tolerant) systems for environments that do not allow access for manual maintenance, such as space, underseas, and other locations (eg, PHM, aircraft), where access is either impossible or excessively costly.

c. Enable almost uninterrupted operation of real-time systems in areas in which manual intervention creates unacceptable delays.

d. Provide the possibility of lower initial costs (for a given reliability goal) than a system that depends on fault avoidance (intolerance). This can occur in cases in which fault tolerance allows use of less costly components or reduces the cost of designed-in fault elimination before the system is delivered.

e. Provide the possibility of reduced life-cycle costs over systems with manual maintenance requirements. Fault tolerance design can reduce maintenance to off-line replacement of disconnected elements, eliminating costs associated with unavailability of systems between the failure and completion of repairs.

f. Provide psychological support to system users through knowledge that fault tolerance is incorporated in the system on which they depend for safety or other benefits.

The full potential of fault tolerance has never been realized. This program focuses on demonstrating this potential.

1.6 Current roadblocks. There are several obstacles to cost-effective application of fault tolerance in military systems:

a. Lack of continuity. Some fault tolerance techniques were developed for first-generation computers but were discarded because the second-generation computer demonstrated a much higher reliability in semiconductor and magnetic-core components. In addition, many solutions were not openly documented, causing much reinvention of techniques. Also, many of the errors were repeated with subsequent loss of confidence in those techniques.

b. Lack of cost/benefit measures. Thus far there are no general methods for a convenient quantitative assessment of the benefits (in terms of life cycle cost reduction) of fault tolerance. The initial extra costs due to the various redundancy techniques is more directly evident and tends to bias a large class of users (who do not have an absolute requirement) in favor of systems without fault tolerance.

c. Lack of specifications and acceptance tests. The user community at large does not have adequate knowledge of the properties and limitations of fault tolerance. As a consequence, specifications for reliability are insufficiently precise and virtually unverifiable in advance of system use. For example, reliability requirements for a given time interval do not specify classes of faults and do not define what constitutes acceptable recovery. Also, the MTBF specifications do not explicitly deal with fault classes (eg, transients and design faults) and recovery requirements, and ignore the differences between redundant and nonredundant designs. Extremely high reliability and MTBF predictions are sometimes offered without stating the implicit assumptions of a static reliability model and a very limited class of faults. In contrast, consider speed requirements in instructions per second, which can be stated and tested for acceptance very precisely.

d. Fragmentation of efforts. Program efforts to increase reliability of systems originate within several disciplines of engineering theory and practice. These include system architecture, software engineering, testing and design verification, design of data base management systems, computer networks and communication systems, component and packaging engineering, field operation and maintenance, and others. Although they all have a common goal, these efforts have remained largely disjointed. A definite lack of common viewpoint and of systematic communication is evident at the present time. There is also a gap between the results of theoretical investigations and practical engineering solutions to fault tolerance problems.

e. Inertia in the design process. Introduction of fault tolerance in system design requires an early commitment and a significant departure from the traditional evolutionary design of system or subsystem "product line" in which compatibility of software is usually a dominant factor. While the number of fault tolerance techniques to serve as maintenance aids has been increasing, none of the major manufacturers has announced a fully fault-tolerant

line of computers or subsystems. The only fault-tolerant systems that have been actually delivered were custom-made to special requirements. The military must provide the impetus to foster wide use of fault tolerance.

f. Resistance to potential impact. Successful introduction of fault tolerance may cause some de-emphasis of several currently profit-making activities. Development of ultra-reliabile devices, maintenance and operations personnel support, new test equipment development, and activities associated with the a priori verification of software are examples of these activities.

In conclusion, while most of the above difficulties are common to many disciplines in systems engineering and science, they reach their greatest severity in the science and implementation of fault tolerance.

1.7 Systems approaches critical. On the basis of the discussion of obstacles, it is clearly imperative that fault tolerance be designed, evaluated, and managed from a total systems viewpoint. All current and proposed efforts must be identified, analyzed, and integrated to achieve the optimum balance in an R&D program plan as well as in those applications involving fundamental tradeoffs between design requirements, life-cycle costs, and maintainability. Appendix B is a summary of current and proposed fault-tolerant systems research and studies. All decisions in specifications and design must be carefully analyzed to determine detrimental effects on other system effectiveness parameters. It is the intent of this program plan to develop understanding of all critical system design parameters and their relationship to one another. It is apparent that the simplest and most effective program will result from a systems-oriented approach.

1.8 R&D strategy. Development of fault-tolerant technology by the military must be in consonance with the efforts of other government, industrial, and university organizations. It is recognized that in a period of austere budgeting for R&D, the military must plan for effective use of its budget to obtain the maximum return. Such a planning strategy is summarized below:

a. The primary objective of this program plan is the development of fault tolerance technology that can be applied to all systems. Although it is feasible to support the development of a fault-tolerant capability in a specific system, generally cost, technical risk, and other specific concerns of technology will not allow specific development of fault-tolerant technology in a system. Unlike NASA, which can spend significant resources to achieve its object in a specific system, the military must focus on developing technology to make it available for a multitude of different systems. This can be achieved through planning that focuses on specific areas of technology while exploiting other research supported by National Science Foundation (NSF), National Aeronautics and Space Agency (NASA), and other governmental and industrial organizations. The objective of this plan should be the funding (seeding) of basic ideas which can lead to larger projects. It should foster the overall technology but use major funding in selected applications.

b. Selected military applications which must be addressed to meet military requirements include electronics/avionics, communications, surveillance, command control, and then more specific areas. Among the specifics include computer netting, human error in systems, data base fault tolerance, fault-tolerant software, and fault/failure prediction in all systems. These areas must be the focus of attention in all demonstrations of capabilities. In a limited budget, the need exists to keep the research directed toward critical application areas. It is also necessary to maintain a management and communication approach that will foster technology transfer.

c. Technology transfer involves several aspects of communications between the technical and management communities. First, the military must provide a means of exchanging information that will advance the technology. One approach is the use of a series of technology workshops that are application (rather than uniquely technology) oriented. Also, the military can develop, maintain, and distribute a series of publications (eg, a handbook on built-in test) that reflect the baseline of the technology. Such a series of state-of-the-art publications has been conspicuously lacking in this area.

In summary, the R&D program in fault tolerance requires a serious commitment from the military. It involves recognition of the need for expertise both within and outside the military community to provide continuity in the technology.

1.9 Specific Requirements

1.9.1 Air Force fault tolerance requirements. The US Air Force has two different sets of requirements for fault-tolerant systems, depending on the availability of maintenance for the system. One set of requirements is represented by manned aircraft and the other by unmanned spacecraft. Typical of the first set of requirements is the tactical aircraft of the 1980s. This aircraft should be able to operate out of a bare base for a 30-day period with the following capabilities:

- Multiple (typically six) sorties/day
- No delay in turnaround time due to maintenance actions
- No aborts due to failure of electronics
- Degraded performance after failures not less than 50% of full-up performance in terms of mission effectiveness
- All faults removed in a single maintenance period per day, usually not more than 6 hours
- No flight-line test equipment
- Maintenance performed with minimum-skill-level personnel

There will be deviations in requirements from those listed above, depending on whether the design is for a tactical fighter aircraft, a strategic bomber, an airlift aircraft, or even a piece of ground equipment, such as a radar. If the requirements enumerated above for the tactical fighter can be solved, significant progress will have been made toward solving the problems of reliability and maintenance for other manned systems. Therefore, a reasonable approach to solving these problems is to study the tactical fighter aircraft and translate the solution for this aircraft to other manned systems. For any of these aircraft the designer must consider an optimum mix of fault tolerance for a short period of time, and quick fault removal when maintenance can be performed.

Requirements for unmanned spacecraft are significantly different from those for manned aircraft. In the case of spacecraft, the emphasis is on highly reliable operation over a long period of time. Typical parameters are 95% probability of successful operation after 5 years in space. In this case toleration of faults is the important, or driving, aspect with little or no emphasis on fault removal. Redundancy techniques that mask failures are acceptable in the spacecraft situation, but not for aircraft where detection, isolation, and removal of faults are required in order to meet the long-term operational goals of the system.

1.9.2 V/STOL aircraft requirements. The V/STOL aircraft represents an advanced concept in naval weaponry, and its successful deployment in the 1990s will require a significant advance in new technology. Current expectations for V/STOL and its use on surface effects ships, DD963, and other ships not designed for carrying aircraft will dictate significant changes in operations and design. An aircraft which must be supported aboard a ship other than an aircraft carrier requires sound, practical logistics support concepts. These new concepts present a challenge to implement new fault-tolerant designs.

The Navy reliability and maintainability requirements for V/STOL are stringent and far exceed current aircraft capabilities. They involve approximately 200% improvement in reliability and a total maintenance time not to exceed 10% of total time, an exacting objective of total maintenance time not to exceed 72 hours of each month. It is recognized that these requirements can only be met by:

- Built-in-test design for fault detection, isolation, and repair
- Extensive use of redundancy for improving reliability and increasing the interval between both scheduled and unscheduled maintenance
- New concepts in partitioning for more improved design between avionics accessibility and in-flight maintenance capability

An expanded fault tolerance technology program is clearly a Navy need for the successful deployment of the V/STOL in the 1990s.

1.9.3 Command control requirements. The continuous and survivable operation of command control systems has been addressed primarily by the use of redundant equipment supported by the backup human element. The integration of man and machines into effective, highly reliable, and highly maintainable systems is a pressing demand. As systems become more complex, the repair (downtime) may increase as well as the operational cost. In a period of decreasing budgets, and with operations and maintenance cost increasing, the design of reliable, easily maintainable equipment remains a critical need.

2.0 Fault Tolerance Program Plan

2.1 System design and acquisition cycle. The ultimate objective in the acquisition of a system or equipment is to achieve maximum utility at minimum cost. The required level of reliability, fault tolerance, and maintainability in systems delivered to the users should be balanced against logistic support complexity and potential life-cycle costs. Acquisition of a system involves a series of phases. During each phase the fault tolerance and other capabilities are enhanced, if appropriate knowledge, technology, and methodology are carefully applied. This R&D program plan is based on supporting the design and acquisition process in achieving fault tolerance.

The acquisition process is depicted in figure 2 as a simple phase-to-phase flow diagram. The transition points denote major achievement milestones which, if attained, signify the successful completion of the preceding phases. Each phase consists of several engineering and management projects. These projects are composed of several tasks, and are listed in appendix A, Project Descriptions. Table 1 establishes the correlation between the program plan objectives (paragraph 1.1) and the projects listed in appendix A.

2.2 Operational requirements. System mission and operational concepts are identified and described in the operational requirements; specifically, the purposes, environments, and operational methods of the warfare and support areas for both the present and foreseeable

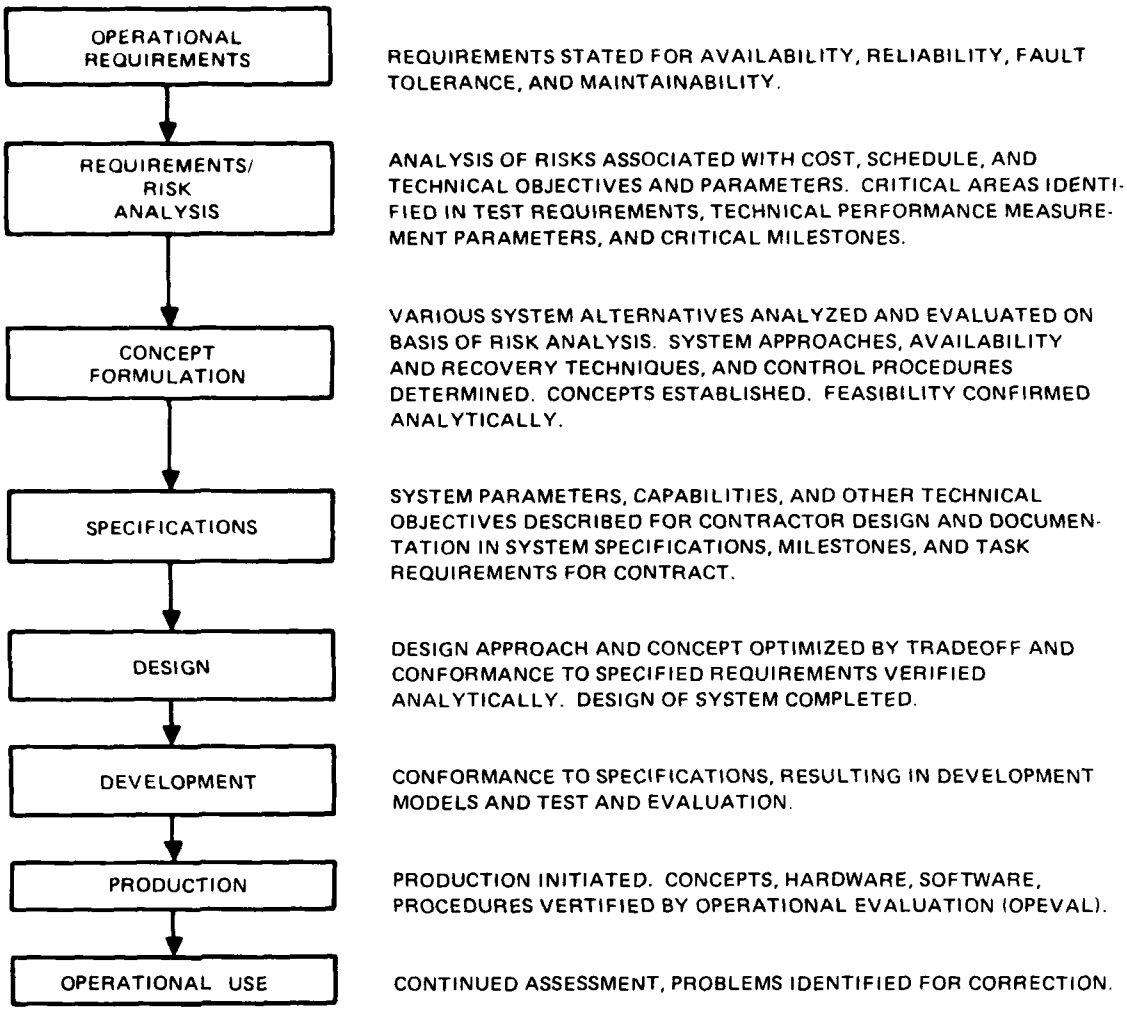


Figure 2. Phases of system acquisition.

future are identified. This includes the operational needs and capabilities in a form for guiding both research and development over a long period of time. Key parameters should be identified and performance goals and cost-performance listed for systems. It is important to describe required capabilities by priority or time urgency, and criticality of failure.

Specific quantitative requirements for fault tolerance are usually not determined from a cursory review of system operational requirements. In fact, fault tolerance is inextricably tied to, or governed by, other system effectiveness parameters. To specifically define fault tolerance requirements, it is necessary to have a clear-cut set of definitions that can be used to derive fault tolerance and can ultimately be quantitatively optimized with respect to other operational factors. Therefore, it is necessary to develop procedures, requirements, and use conditions for achieving the following objectives:

a. Establish baseline requirements for fault tolerance which are amenable to design interpretation and implementation. There should be a set of definitions, terminology, and other supporting concepts provided for the development of specifications and procurement documents.

TABLE 1. PROJECT TO PLAN OBJECTIVE CORRELATION.

Project Description	Plan Objective		
	A	B	C
Fault Tolerance Requirements Definition and Interpretation	X		
Mission Availability Analysis Methods	X		
Project DAIS Fault Tolerance Evaluation	X		
Relation of Requirements to Specification	X		
Reliability/Fault Tolerance Analysis and Design Tools		X	X
Alternate System Design Evaluation			X
Fault Tolerance Life-Cycle Cost Impacts- Maintenance Model			X
Establishment of Redundancy Limits/Tradeoffs		X	
Theory of Testing Taxonomy			X
Reliability-Measure of Testability Concept			X
Failure-Fault Prediction Technology		X	
Recovery Techniques		X	
Transient Faults		X	
Identification of Failure Modes		X	
Fault-Tolerant Software		X	
High-Order Language Constructs For Fault-Tolerant Systems			X
Analog Functional Redundancy		X	
Functional Test Design Theory			X
Fault Tolerance -Validation and Verification			X
Estimation of Confidence Limits Testing Large Logic Networks		X	
Command Control Fault Tolerance	X		
Architectures For Availability Requirements	X		
Communication Protocol For Fault Tolerance			X
Specification For Redundancy Management	X		
Standards and Fault Tolerance	X		X
Self-Diagnosing Design Techniques	X	X	
Redundant Microcomputers		X	
Loosely Coupled Fault-Tolerant Computer Networks		X	
Fault Tolerance Masking Hazards		X	X
Fault Tolerance Design Handbook	X	X	X
Design/Development Tools (Methodology)	X	X	
Acceptance Testing		X	X
TECHEVAL-OPEVAL Techniques	X		X

Plan Objective:

A. Clarify operational requirements and relate them to system specifications.

B. Establish alternate system design method for balancing operational capabilities against life-cycle costs.

C. Develop understanding of system engineering relationships between reliability, fault tolerance, repairability, and logistics support.

b. Define a firm basis of demonstration test plans and criteria for acceptance testing. Development of validation and verification plans begins with the clear definition of requirements in terms of quantifiable parameters.

c. Provide a basis for establishing and applying appropriate formal management controls that can be used at designated critical milestones. Management of systems acquisition with a high technology requirement is important and dependent on the quantification of parameters.

d. Provide a quantifiable, realistic baseline for life-cycle cost analysis and logistic support planning.

All the above objectives depend on clear definition of requirements in quantifiable parameters. Therefore, the following projects are required in the area of requirements definition.

- FAULT TOLERANCE REQUIREMENTS DEFINITION AND INTERPRETATION

The purpose of this task is the development of a more meaningful method of describing maintainability and reliability which will result in the effective application of appropriate fault tolerance technology. Current technology utilizes terms such as MTBF, MTTR, and NORM, but in fact does not consider degrees of tolerance, on-line versus off-line, man-machine tradeoffs, etc. This project will explore the best means of describing reliability and maintainability requirements for greatest effectiveness.

- MISSION AVAILABILITY ANALYSIS METHODS

This project addresses mission analysis tools and techniques, emphasizing their relationship to fault tolerance. The project proposes, through several interrelated tasks, to evaluate existing automated aids for fault tolerance requirements analysis, and then to utilize these tools in demonstrating tradeoff analysis in selection, degree of fault tolerance, on-line versus off-line application, etc.

- PROJECT DAIS FAULT TOLERANCE EVALUATION

The AF DAIS program established and designed to meet specific reliability goals. The project will conduct an analysis of the DAIS system to determine its effectiveness in meeting its realiability goals. This project will determine the adequacy of the specifications, requirements, and design in the system acquisition process.

2.3 Requirement/risk analysis. The analysis of requirements to determine risks associated with costs, schedule, objectives, and technical parameters is required for a successful acquisition program. It should identify technical performance measurement parameters, test requirements, and critical milestones. The analysis will require a quantifiable foundation of the technical and physical characteristics for a fault tolerance technology (also reliability, maintainability, and supportability). In order to perform the analysis, certain necessary automated analysis design tools will be required. Those that are not available must be developed. This phase of the acquisition process is the foundation for technical program planning and control. Definition of effective and total systems programs requires that present analysis capabilities be strengthened. The enhanced capabilities are critical for tradeoff of objectives in selection of the concept formulation. The following broad R&D projects are required for development of a quantifiable foundation of design analysis for physical and technical characteristics of fault tolerance technology.

· RELATION OF REQUIREMENTS TO SPECIFICATION

This project, through a series of interrelated subtasks, will define, relate, and formulate specifications necessary for achieving a given set of operational requirements and provide design tools for use in designing fault-tolerant systems. It will relate the defined requirements to an identified set of specifications that are critical in meeting requirements. This project will review the process of developing requirements, performing risk and cost analysis, concept formulation, and design specification.

· RELIABILITY/FAULT-TOLERANT ANALYSIS AND DESIGN TOOLS

The goal of this project is to reduce the complexity of the mathematical model and the associated programs while retaining the ability to represent and investigate a wide variety of redundant systems configurations. Within the area of investigation is ARIES (Automated Reliability Interactive Estimation System), which is an interactive package of programs for computer-aided reliability analysis of fault-tolerant redundant systems. This project should present a unified viewpoint of reliability modeling based on the theory of finite-state, continuous-time Markov processes. The project should develop a structured, integrated approach that will be broadly accepted by the practitioners in the field.

· FAULT TOLERANCE LIFE-CYCLE COST IMPACTS – MAINTENANCE MODEL

The relation of fault tolerance to both acquisition and life-cycle costs has not been clearly understood and this task is intended to develop the relational structure. This task involves the analysis and development of maintenance and support models based on the relational structure.

· REDUNDANCY LIMITS/TRADEOFFS

The objective of this project is to establish how much redundancy is required to meet the fault tolerance objectives of system design. Graphical and analytical approaches will be used to establish the amount of redundancy needed for a particular design.

2.4 System concept formulation. This phase of the system acquisition cycle begins with stated system operational requirements, mission objectives, environmental factors, technical performance, and system figures-of-merit as stipulated and proposed, and examines the validity, consistency, desirability, and attainability of system approaches with respect to current technology, physical resources, human performance capabilities, life-cycle costs, and other constraints. System functions and subfunctions are identified and analyzed as a basis for identifying alternatives for meeting performance and other requirements. Each function and subfunction is allocated to each requirement by conducting selected analysis, synthesis, and design activities. This phase of the design and acquisition cycle should produce a set of system design specifications for contract. System concept formulation activities logically partition into the following areas for more detailed discussion:

a. Functional definition. Functional definition for fault tolerance will determine modes of operation, reliability required for system functions and subfunctions, fault tolerance functional partitioning, operational usage and support, and other system functions. Performance requirements are established for each function, and subfunctions are identified. Timing allocation is analyzed and defined. Time requirements that affect mission success, safety, and availability are derived. Sufficient detail should be available to allow specification of hardware, software, procedural data, and personnel. All functions and their distribution must be traceable through analysis to the system operational requirement they are designed to fulfill.

b. System approaches. Given a functional description, various systems approaches can be explored relative to meeting system requirements, costs, and other objective tradeoffs.

Sufficient preliminary design and analysis to confirm and assure the completeness of performance are necessary. In addition, the configuration and its arrangement of the elements of system are explored. Techniques for detection, isolation, recovery and repair, and operation are portrayed in a suitable form to illustrate system and item interfaces, traceability between elements, and documentation of basic source data for project management and control. This phase is also concerned with logistics engineering, life-cycle costs, and optimization of alternative approaches.

The following tasks are needed to develop the system concept formulation of fault tolerance.

- THEORY OF TESTING TAXONOMY

The goal of this project is to develop a new understanding and application of testing techniques to fault-tolerant systems. The theory of testing has always been an area of confusion with no common definition. There is uncertainty as to how much testing is enough and what is the relative applicability of a given testing technique. With complex systems in the field, experience is indicating that life-cycle costs are dominating procurement costs, and testing and maintenance are the major sources of life-cycle costs as well as a limiting factor of performance due to system availability.

- RELIABILITY MEASURE OF TESTABILITY CONCEPTS

The goal of this project is to formulate a fundamental unit to measure the testability of circuits, subsystems, and systems.

A fundamental quantifiable parameter that is a measure of testability of the system would allow a hierarchical structure to be developed. Such a structure could identify areas requiring more extensive testing, the points on partitions at which verification could be difficult. It is critical to the design and acquisition process that a quantification of testability be developed.

- FAILURE-FAULT PREDICTION TECHNOLOGY

This project addresses the development of the techniques, concepts, and methodologies for fault/failure predictions. It will encompass both analog and digital fault prediction and the system approaches necessary to exploit the capability of prediction.

The advance of microelectronic technology will permit the monitoring and analysis of circuit and system parameters for fault and failure prediction. This capability will allow tremendous savings in maintenance and retrofit costs in addition to significantly improving the fault tolerance performance of systems.

- RECOVERY TECHNIQUES

The purpose of this project is to develop system design approaches for effective application of recovery techniques to fault-tolerant systems. Recovery techniques in fault-tolerant systems are implemented to compensate for detected faults, and these techniques are germane to successful system design. In their simplest form they consist of voter circuits, and in the more complex systems they are extensive and complicated software programs.

- TRANSIENT FAULTS

Transient faults that occur in electronic systems have been difficult to cope with because of their elusive nature. This project will address the nature of transient faults and the test techniques that are applicable for detection.

Transient faults are serious because they introduce errors at the least desirable time, which can be catastrophic. In the past such faults were accepted as undetectable and impossible to isolate. However, recent advances in technology indicate that such faults can be detected and corrected.

· IDENTIFICATION OF FAILURE MODES

The goal of this project is to identify and classify failure modes that are likely to occur in the various classes of systems. A fault-tolerant design must be based on statistical failure rates. For this reason failure rate data must be collected and categorized.

· FAULT-TOLERANT SOFTWARE

It is the goal of this project to develop a theoretical foundation for detecting, isolating, and recovering from faults with reliable software.

Reliable software implies robustness of fault tolerance. That is, it is expected to deliver a certain minimum level of services even when faced with an unexpected or hostile environment (such as hardware failure or bad data). Techniques for detection and isolation of faults are classified into testing (analysis of responses of a selected set of input data) and verification (mathematical proof and constructive approach).

· HIGH-ORDER LANGUAGE CONSTRUCTS FOR FAULT-TOLERANT SYSTEMS

The purpose of this project is the analysis and development of fault-tolerant language constructs suited for inclusion in the DoD high-order language standard.

This project will address language constructs that allow incorporation of program redundancy into a block-structured program in a well structured manner. This project does not address system architecture and design methodologies for fault-tolerant programs.

The most effective method of meeting complex availability requirements and reducing development and support costs is to develop methodologies and tools for systematic incorporation of redundancy programming in a well structured form. Good structuring of a fault-tolerant program is particularly important, since the use of program redundancy increases program size. Fault-tolerant programs have generally higher development costs and higher processing cost. The high processing cost of fault-tolerant programs is due to increased processor time and increased storage space required for executing redundant program components.

· ANALOG FUNCTIONAL REDUNDANCY

This project will address several approaches that will result in the use of functional redundancy in analog circuits and will define structuring of analog fault tolerance test techniques and capabilities, and also those characteristics of analog circuits that can be exploited in systems. The analog circuits to be considered will span the entire known frequency range, will be of both high and low power, and will represent a complexity of functions rivaling the ability of digital circuits.

Analog circuits provide a unique challenge to fault-tolerant design since they are particularly complex and are far more prone to failure than digital circuits. Analog circuits often require tight component tolerances to function properly and tend to slowly degrade. This slow degradation presents a special challenge to the designer of redundant circuits.

· FUNCTIONAL TEST DESIGN THEORY

This project will develop the theory of functional testing, from its theoretical foundations to principles of application in systems, software, and hardware. This program can become the basis of functional testing microcomputers as well as analog functional testing.

Functional testing has often been omitted in system design until the last stages. This leads to testing as an add-on, rather than a built-in, function. If a good applied theory of testing is developed, functional testing can become part of design from the beginning.

· FAULT TOLERANCE VALIDATION AND VERIFICATION

This project will address the validation and verification problem from the perspective of the systems acquisition manager, beginning with operational requirements and proceeding through systems acceptance test and evaluation.

Without verification procedures it will be difficult, if not impossible, for the government to put a fault tolerance requirement into a system specification. There must be a clearly defined procedure for the government to use in purchasing a system from a contractor; otherwise the fault-tolerant specifications can only be design goals and not design requirements.

- ESTIMATION OF CONFIDENCE LIMITS TESTING FOR TESTING LARGE LOGIC NETWORKS

The purpose of this project is to provide a methodology and means for accurately determining confidence limits for the reliability of large digital logic networks, without exhaustively exercising all possible input sequences or simulating all logical faults in the network. The project addresses development, implementation, and demonstration of a logic simulation and fault analysis system to serve as a tool for determination of reliability confidence limits in digital networks containing up to 15 000 elements.

Faults will be modeled via probabilistic techniques, and will occur singly and in multiple. The system, when completed, should be capable of reasonably approximating the actual operation of an existing logic network, including occurrence and location of failures, when all necessary processing and operating parameters are input to the model. As long as the built-in redundancy has not been exhausted, no symptom will appear outside the module. However, when the redundancy has been exhausted or overwhelmed by a fault, module failure will result. Separate detection and recovery functions are not identified from outside the module.

- COMMAND CONTROL FAULT TOLERANCE

The goal of this project is to develop a design and evaluation methodology for fault-tolerant command control global networks.

The availability of the military C^3 systems on a global basis is of major importance, especially during the periods preceding and during a conflict. A fault-tolerant design could contribute to the availability of a system during critical periods.

Because of the many sensors now available, the sophisticated data processing, and the man-machine interfaces required, it is critical that fast communications be available within a platform, among platforms, and on a global basis to give a commander critical information when he needs it. This is true during the entire conflict scale, from a prehostilities crisis to global war, because data acquired from local sensors as well as from those operated by shore-based commanders in support of task forces will be correlated and evaluated in near real time as inputs to a commander's decision-making process.

- ARCHITECTURES FOR AVAILABILITY REQUIREMENTS

The purpose of this project is the review, analysis, and development of system architecture and networks that will result in increased fault-tolerant systems capabilities. Through this project, system architecture tradeoffs will be established and applied to determine practical system structures that meet all requirements.

The importance of this project is reflected in the fact that system architectures for meeting performance designs are in conflict with those of fault-tolerant design (eg, performance design dictates single centralized processing while fault-tolerant design requires distributed processing and multichannel communications).

- COMMUNICATION PROTOCOL FOR FAULT TOLERANCE

Bus protocol for reconfigurability of bus structured system architecture is necessary for simple and cost-effective system design. This project addresses the requirements and specifications that lead to standardization of bus protocol. It will review, analyze, and catalog existing and proposed bus protocols and interface techniques to determine fault-tolerant systems applicability.

2.5 Specifications. After the system concept has been formulated, system specifications need to be written. The contractual requirements of a potential supplier require careful definition to ensure that acceptance by the government will be accomplished smoothly.

The specifications should include the system design requirements and goals, the acceptance procedures, the documentation requirements, the major milestone requirements, and any other data that may be required by a particular procurement.

The following projects are required for fault tolerance specifications development.

· REQUIREMENTS FOR REDUNDANCY MANAGEMENT

The goal of this project is to develop a common approach to fault-tolerant system design through redundancy management. First there will be an analysis of fault-tolerant redundancy design techniques and management techniques will be developed.

· STANDARDS AND FAULT TESTING

The goal of this project is to recommend changes to existing military standards that include fault-tolerant designs. The use of standards is necessary for simplified and cost-effective application of fault tolerance in military systems. This task will be instrumental in obtaining a fault-tolerant capability in all military systems.

2.6 Design and development. Design is the process by which the conceptual approach is optimized through tradeoffs and conformance to specifications. It involves analytical verification and specific system synthesis and implementation. This phase of the acquisition cycle involves many different areas:

a. Translate specifications to hardware/software. Evolve a detailed design conforming to specified fault tolerance requirements, system fault-tolerant concept, and demonstration requirements.

b. Conduct fault-tolerant analysis and design evaluation, to guide mechanization process.

c. Assess fault-tolerant capability in final design configuration and compatibility with a specified fault tolerance concept.

d. Incorporate all specifications and tasks into an integrated systems product for final development.

In support of these design areas the following broad, all-encompassing R&D projects should be accomplished.

· SELF-DIAGNOSING DESIGN TECHNIQUES

The goal of this project is to develop a definition of general specifications for design and utilization of LSI components and modules in self-diagnosing systems.

This project will study and analyze architecture, functional partitioning, and module and component design features necessary for achieving self-diagnostic microprogrammable capabilities in processors. The project will result in a set of guidelines for designing LSI components and modules that ensure testability of the component and the system employing the component. Redundancy levels, organization of functions, requirements for test points to be made accessible, and the procedures for using these data to design and implement a processor that is self-diagnosable down to the replaceable module level will be postulated and verified.

· REDUNDANT MICROCOMPUTERS

The purpose of this project is review, analysis, and development of redundant microcomputer concepts for fault-tolerant systems design.

The advent of the one-chip microcomputer has opened the possibility of new approaches to redundant computer configurations that exploit hardware executives, simplified voting circuits, and reduced switch complexities. The use of redundant microcomputers is now considered cost-effective and feasible for broad classes of problems. This project will formalize the approaches to applying redundant computers through analysis, design, and verification.

· LOOSELY COUPLED FAULT-TOLERANT COMPUTER NETWORKS

The objective of this project is to develop a theory that will address the problems of loosely coupled computer networks. Loosely coupled computers are defined as those between any two of which there is only one-way communication. Often a system (for example, the command control system) has long distances between its various subsystems and, due to these long distances, the communication paths have large delays. If a message is not received correctly, it is impractical to immediately notify the sender to repeat the message. This constraint on the system presents new problems that may require changes in design in order to make the system fault-tolerant.

· FAULT TOLERANCE MASKING HAZARDS

The goal of this project is to investigate contemporary problems associated with redundancy, in particular those associated with masking (or static redundancy), and to develop a set of design guidelines that will help designers avoid problems in designing with static redundancy.

· FAULT TOLERANCE DESIGN HANDBOOK

The summation of technological data on fault tolerance technology should be contained in a fault tolerance design handbook, and this task will develop the handbook to assume the widespread dissemination of data.

· DESIGN/DEVELOPMENT TOOLS (METHODOLOGY)

Design and development of complex fault-tolerant systems involve many procedures, techniques, and methods that can be automated. In particular, tools can be automated for generation of tests, documentation, circuit simulation, and other functions. This project will address the development of the design and development methodology and the tools required to support it.

2.7 Test and evaluation. System acquisition generally requires that an Initial Operational Test and Evaluation (IOT&E) be conducted in order to validate the reliability and maintainability characteristics of a system. IOT&E design requires that special consideration must be given to fault-tolerant systems, since internal failures may be masked by the designed-in fault-tolerant characteristics of the system. There is a requirement to account for, measure, and document these internal failures. An internal failure will degrade a system and make it less fault-tolerant; however, it is generally unobservable from outside the system. Therefore, IOT&E specifications will require special provisions for testing and evaluating fault-tolerant systems. The following projects address these problems.

· ACCEPTANCE TESTING

The goal of this project is to develop acceptance testing procedures for fault-tolerant systems. Fault-tolerant systems continue to operate normally even though there has been a failure. However, the failure will have degraded the system. Therefore, special acceptance testing procedures will be required for acceptance testing of fault-tolerant systems.

· TECHEVAL-OPEVAL TECHNIQUES

The technical and operational evaluation of fault-tolerance capabilities is critical to the development of new systems. Yet, the test and evaluation is difficult to accomplish after system design. The purpose of this project is (a) to access the effectiveness of T&E after-design, and (b) to indicate techniques to perform more effective fault tolerance systems test and evaluation.

3.0 Project Priorities

3.1 Criteria for project selection. The basic objectives of the program plan are (1) to develop the basic foundation of fault tolerance technology, (2) to develop technology particular to the major application/mission areas, and (3) to develop a technology transfer. These represent the basis for the selection of project priorities. Each project is critical to, and relates with, other projects that, in total, meet the program objectives. It is necessary to recognize that not all projects can be accomplished concurrently. Additionally, if they are performed out of sequence, they may not be effective in developing a basic fault-tolerant technology, even if the research has been performed well. If the time priority is not followed, much of the research will need to be repeated at a later date.

The priority list is also important in the selection of tasks during periods when funding is austere. Progress can be made toward the final objective despite funding/fiscal variations.

3.2 Priority list. Table 2 is a list of projects, indicating recommended priority for accomplishment.

TABLE 2. PROJECT PRIORITY.

Project	Priority 1	2	3
I. OPERATIONAL REQUIREMENTS			
1. Fault Tolerance Requirements Definition and Interpretation	X		
2. Mission Availability Analysis Methods	X		
3. Project DAIS Fault Tolerance Evaluation	X		
II. REQUIREMENTS/RISK ANALYSIS			
1. Relation of Requirements to Specification	X		
2. Reliability/Fault Tolerance Analysis and Design Tools		X	
3. Alternate System Design Evaluation			X
4. Fault Tolerance Life-Cycle Cost Impacts - Maintenance Model	X		
5. Establishment of Redundancy Limits/Tradeoffs			X
III. SYSTEM CONCEPT FORMULATION			
1. Theory of Testing - Taxonomy	X		
2. Reliability-Measure of Testability Concept	X		
3. Failure-Fault Prediction Technology		X	
4. Recovery Techniques			X
5. Transient Faults			X
6. Identification of Failure Modes			X
7. Fault-Tolerant Software		X	
8. High-Order Language Constructs For Fault-Tolerant Systems	X		
9. Analog Functional Redundancy		X	
10. Functional Test Design Theory	X		
11. Fault Tolerance - Validation and Verification	X		
12. Estimation of Confidence Limits Testing Large Logic Networks		X	
13. Command Control Fault Tolerance	X		
14. Architectures For Availability Requirements		X	
15. Communication Protocol For Fault Tolerance		X	
IV. SPECIFICATIONS			
1. Specification For Redundancy Management		X	
2. Standards and Fault Tolerance	X		
V. DESIGN			
1. Self-Diagnosing Design Techniques	X		
2. Redundant Microcomputers		X	
3. Loosely Coupled Fault-Tolerant Computer Networks			X
4. Fault Tolerance Masking Hazards			X
5. Fault Tolerance Design Handbook		X	
6. Design/Development Tools (Methodology)	X		
VI. TEST AND EVALUATION			
1. Acceptance Testing	X		
2. TECHEVAL-OPEVAL Techniques	X		

Priority: 1 Immediate need
2 Important
3 Less critical

APPENDIX A:
PROJECT DESCRIPTIONS

SECTION A1.

OPERATIONAL REQUIREMENTS PROJECTS

FAULT TOLERANCE REQUIREMENTS DEFINITION AND INTERPRETATION

1.0 Introduction (objective). The purpose of this task is the development of a more meaningful method of describing maintainability and reliability which will result in the effective application of appropriate fault tolerance technology. Current terminology utilizes terms such as MTBF, MTTR, and NORM, but in fact does not consider degrees of tolerance, on-line versus off-line, man-machine tradeoffs, etc. This project will explore the best means of describing reliability and maintainability requirements for greatest effectiveness.

2.0 Approach. This task will compile a set of terminology and relate the terms to fault-tolerant parameters.

3.0 Scope. This task is limited only to requirements definitions. It must be integrated with other tasks on risk analysis and fault tolerance specifications.

4.0 References

5.0 Background

MISSION AVAILABILITY ANALYSIS METHODS

1.0 Introduction (objective). The force structure analyses upon which the military bases its major procurement decisions involve force effectiveness calculations that generally assume command control functions are carried out to perfection with perfectly operating equipment. However, in practice, when equipment fails, redundancy may or may not exist, and the resulting performance is far from ideal. A good mission exercising capability must be provided to exploit the development of fault-tolerant technology in command control and other systems. The nature of redundancy, its requirements and relationship to mission availability, and its dependence on new technology must be understood. Tools must be provided to achieve automated assistance in availability analysis. Particularly important in these analyses is the impact of human errors that often may affect combat readiness.

2.0 Approach. This project will consist of the interrelated tasks listed below.

2.1 Evaluation of automated aids for fault tolerance requirements analysis. Various existing programs will be compared, advantages and disadvantages listed, and recommendations for mission availability analyses programs presented.

2.2 Experimental mission availability analysis. This task will utilize the tools developed in paragraph 2.1 above and demonstrate tradeoff analysis in the selection, degree of fault tolerance, on-line versus off-line, role of the human, etc.

3.0 Scope. This project will address only the mission analysis tools and techniques and their relationship to fault tolerance requirements.

4.0 References

- Project TRANSIM, A Ten-Year Progress Report, RR O'Neill and AM Feiler, UCLA-ENG-7448 August 74, contract N00014-69-A-0200-4052
- Carrier Aircraft Support Effectiveness Evaluation (CASEE), A Report, NAVAIRSYSCOM-AIR-52022, 2 June 1976
- ANALOG ATG Research at Grumman, HH Schrieber, 24 March 1977, to be presented at the National Aeronautical and Electronics Conference
- A Study of the Recoverability of Computing Systems, Merlin, PM Univ Microfilms, Ann Arbor, MI, no 75-11026, Univ of California, Irvine
- Recoverability of Modular Systems, Merlin, PM, Farber, DJ, Proceedings of the ACM Sigcomm/Sigops Interprocess Communications Workshop, p 51-56, 24-25 March 1975, ACM, NY

5.0 Background. Military systems such as a Navy task force or aircraft carrier performance in a given mission will experience different decision-making situations that are dependent on the availability of different equipment. Current methods of analysis need to be supplemented by automated methods based on well formulated models.

PROJECT DAIS FAULT TOLERANCE EVALUATION

1.0 Introduction (objective). The AF DAIS program was established and designed to meet specific reliability goals. The project will conduct an analysis of the DAIS system to determine its effectiveness in meeting its reliability goals. This project will determine the adequacy of the specifications, requirements, and design in the system acquisition process.

2.0 Approach. This task will involve analyzing test data and comparing these data against specification and requirements.

3.0 Scope. The task must be conducted from the point of view of the program manager interested in meeting his project goals.

4.0 References

5.0 Background

SECTION A2.

REQUIREMENTS/RISK ANALYSIS PROJECTS

RELATION OF REQUIREMENTS TO SPECIFICATION

1.0 Introduction (objective). This project will define, relate, and formulate the specifications that are necessary to achieve a given set of operational requirements. It will identify a lexicon for stating the operational requirements for availability. It will relate these requirements to an identified set of specifications that are critical to meeting the requirements. This program will review the process of developing requirements, performing risk and cost analysis, concept formulation, and design specification.

2.0 Approach. The following tasks are to be performed:

2.1 Operation requirements definition. This task will define a set of operational requirements. The lexicon will include a degree of fault tolerance, operational procedures, and other specific requirement description.

2.2 Specification definition. This task will define a set of specifications for fault-tolerant design that can be related to the operational requirements, and the system concept formulation process.

2.3 System concept formulation definition. This task will address the definition of three areas: operating procedures, system approaches, and availability and recovery. The importance of these areas to unambiguous specifications for fault tolerance is recognized. Each of these areas must be addressed separately and then all must be addressed collectively.

3.0 Scope. This project should relate the requirements-specification relationships to the military procurement procedures. This will include all aspects from initial specification to the retirement of the system.

4.0 References

- A Fault-Tolerant Estimator for Redundant Systems, Broen, RB, IEEE Transaction Aerosp and Electron Sypt, vol AES-11, no 6, p 1281-1285, November 1975, McDonnell Aircraft Co
- Approaches to Reliable Computing, Avizienis, A, Sigplan-not, vol 10, no 6, p 458-464, June 1975, UCLA

5.0 Background. There has been work done on the theory of fault tolerance, but theoretical work has not been, except possibly in a few cases, translated into system specifications so that a contractor can use them to design a system. This project will provide a step in the direction of translating theory into practice.

RELIABILITY/FAULT TOLERANCE ANALYSIS AND DESIGN TOOLS

1.0 Introduction (objective). The goal of this project is to reduce the complexity of the mathematical model and the associated programs while retaining the ability to represent and investigate a wide variety of redundant configurations of systems.

2.0 Approach. A number of different analysis tools need to be evaluated. Within the area of investigation is ARIES (Automated Reliability Interactive Estimation System), which is an interactive package of programs for computer-aided reliability analysis of fault-tolerant redundant systems. This project should present a unified viewpoint of reliability modeling that is based on the theory of finite-state, continuous-time Markov processes. The project must develop a structured, integrated approach that will be broadly accepted by the practitioners in the field.

3.0 Scope. This project must be considered in relation to other design and analysis tools, and every attempt should be made to integrate the analysis and design tools into a larger set of programs which can be used in system analysis and design.

4.0 References

- AIRES An Automated Reliability Estimation System for Redundant Digital Structures, Ying-Way Ng and Algirdas Avizienis, Proceedings 1977 Annual Reliability and Maintainability Symposium, p 108-113
- The Influence of Software Structure on Reliability, Parnas, DL, Sigplan Not, vol 10, no 6, p 358-362, June 1975, Tech Univ, Darmstadt, Germany
- Survey of Computer Reliability Studies, McCluskey, EJ, Ogus, RC, Electro-Technol (India) vol 19, no 4, p 82-95, December 1975, Stanford University
- On Balancing Hardware - Firmware for Designing a Fault-Tolerant Computers Series, Courtois, B, Savcier, G, Micro 8: Workshop on Microprograms, 8th Annual Proc, Chicago, IL, p 1-5, September 21-23, 1975, New York, NY 195
- Reliability and Coverage Analysis of Nonrepairable Fault-Tolerant Memory Systems, Cox, GW, Carroll, BD, Final Technical Report, 1 July 1976, Auburn University, AL, contract NAS8-26930

5.0 Background. Critical to the specification and design of fault-tolerant systems is the availability of analysis tools for the estimation of reliability of fault-tolerant structures. The diversity of possible redundant structures complicates the problem of reliability and availability assessment. Reliability modeling is one of the principal tools for reliability prediction of redundant structures. Because of the extensive computing involved in making an estimate for a single set of parameters, mathematical models of redundant (analog and digital) systems are practically useful to designers only when they are automated in the form of a computer program. Given such capability, the designer (as well as the program manager) can generate numerous reliability predictions and thus explore the sensitivity of the proposed design with respect to changes in various designer-controlled structural parameters. An interactive capability allows new sets of parameters to be entered at some computer terminal and can result in an extensive exploration of design alternatives.

ALTERNATE SYSTEM DESIGN EVALUATION

1.0 Introduction (objective). This project will develop the rationale and procedures for evaluating the relative cost-effectiveness of alternate fault-tolerant system designs. System operational capabilities will be assigned relative values and the cost of providing the various combinations of the capabilities will be compared to their value to the users.

2.0 Approach. A way to relate value to the user and life-cycle cost of a system needs to be developed. This will give a measure of relative cost-effectiveness between alternate designs. It is possible that gaming theory and linear programming may be necessary to arrive at the most cost-effective systems with a given funds constraint. Once the basic evaluation framework is designed, it may be possible to write a computer program to do the evaluation of any system.

3.0 Scope. This project will combine existing data and methodologies with new procedures to measure the cost-effectiveness of alternate system designs.

4.0 References

- Fault-Tolerant Computing: An Introduction, A Avizienis, Computer Science Department, University of California, Los Angeles, January 22, 1977
- A Fault-Tolerant Spacecraft, Gilley, GC, Digest of the 1972 International Symposium on Fault-Tolerant Computing, p 105-109, June 19-21, 1972
- Theory of Games and Statistical Decisions, D Blackwell and MA Girschick, John Wiley and Sons, 1954

5.0 Background. The government needs a procedure for evaluating the cost-effectiveness of alternate fault-tolerant system designs that includes the many constraints that surround government procurement. If this procedure is developed, a clearer direction of effort will guide both the government and contractors in development of better fault-tolerant designs.

FAULT TOLERANCE LIFE-CYCLE COST IMPACTS – MAINTENANCE MODEL

1.0 Introduction (objective). The relation of fault tolerance to both acquisition and life-cycle costs has not been clearly understood and this task is intended to develop the relational structure. This task involves the analysis and development of maintenance and support models based on the relational structure.

2.0 Approach. Develop a set of relational mathematical models for performing cost, availability, and reliability studies of systems using fault-tolerant techniques.

3.0 Scope. The task must be conducted from the point of view of the program manager and system engineer who is faced with the decision on whether to incorporate fault tolerance capabilities.

4.0 References

5.0 Background

ESTABLISHMENT OF REDUNDANCY LIMITS/TRADEOFFS

1.0 Introduction (objective). The objective of this project is to establish how much redundancy is needed to meet the fault tolerance objectives of the system design.

2.0 Approach. The approach will be to develop a graphical and analytical method to determine the amount of redundancy needed to meet the system design requirements for fault tolerance. This will include optimization techniques which will show the tradeoffs between alternate designs.

3.0 Scope. This project will encompass all aspects of fault-tolerant system design.

4.0 References

- Theory of Fault-Tolerance -- 1976 Annual Report, vol I and II, Jack, LA, et al, ONR contract N0014-75-C0011, December 7, 1976
- Fault Tolerance in Galois Trees – An Algorithm for Detection and Location of Stuck-At Type Errors in Trees of Galois Linear Modules, Marver, JM, June 1975
- Reliability Modeling and Analysis of General Modular Redundant Systems, Mathur, FP, Desousa, PT, IEEE Transaction Reliab, vol R-24, no 5, p 296-299, December 1975, University of Missouri

5.0 Background. There is a need to establish design guidelines for the amount of redundancy used to meet a given fault tolerance requirement.

SECTION A3.

SYSTEM CONCEPT FORMULATION PROJECTS

THEORY OF TESTING – TAXONOMY

1.0 Introduction (objective). The goal of this project is to develop a new understanding and application of testing techniques to fault-tolerant systems. The design process, tools, and techniques should be identified. In addition the impact of life-cycle costs should be addressed.

2.0 Approach. The top-down approach requires a foundation in several areas.

2.1 Measure of testability. The measure (or measures) should provide a quantitative assessment of the desired testability. It requires both basic and applied research in analog, digital, and system testability. It would be directed at determining how much testability is possible and what the incremental costs are for a given technique. A framework would be developed to provide a standard way of specifying the degree of testability, isolation, maintainability, and reliability of a system.

2.2 Classification of techniques. Although there are presently a large number of testware techniques available, little or no classification of these techniques exists for fault tolerance or maintainability design. A comprehensive taxonomy would substantially improve application of current knowledge and refine existing techniques.

New research in techniques will be needed to keep abreast of advances in component, device, and systems technology. A structure taxonomy to meet changing demands is critical.

2.3 System engineering approaches. Designing testable systems requires a quantitative theory that allows the system engineering approach to tie fragmented design issues and techniques together. The theory of testing should provide an overall structure for assuring that correctness and verification can be obtained. Integration of testware must be accomplished by application of the theory during the system development cycle.

2.4 Design tools. The tools must provide the mechanism that will allow theory to be applied. The tools will support the program manager and designer during the design and acquisition cycle of the system. This would provide automated documentation, simplified design, and time/cost-effective application of testware techniques.

3.0 Scope. This project is the structure that provides the framework for a large number of testing projects. Its intent is to clearly establish a baseline for testing.

4.0 References

- Theory of Fault-Tolerance, vol I and II, Larry Jack, Honeywell Report, contract N0014-75-C-0011, December 1976
- Fault Detection in Redundant Circuits, Friedman, AD, IEEE Transactions on Electronic Computers, vol EC-16(1)
- Current Research, McCluskey, EJ, Wakerly, John F, Ogus, RC, Technical Report no 100, October 1975, Center for Reliable Computing, Stanford University

5.0 Background. The theory of testing has always been an area of confusion with no common definition, uncertainty as to how much testing is enough, and many questions relative to testing technique applicability. The military needs to formulate the theory of testing and support this theory with a formal structure. The theory should result in new understanding and application of testing techniques. Among the areas that can benefit from a vigorous theory of testing are specifications, design process, tools, and techniques.

Until recently, system testing and support, much like software, have been considered to be of secondary importance in comparison to the major costs of hardware procurement. With complex systems in the field, experience indicates that life-cycle costs are dominating procurement costs. Testing and maintenance are the major sources of life-cycle costs, as well as a limiting factor for performance due to system availability. Brute-force application of test techniques is now recognized as generally ineffective and costly, and a top-down methodology approach to the design and application of testing systems with minimal cost impact is required.

RELIABILITY-MEASURE OF TESTABILITY CONCEPT

1.0 Introduction (objective). This project will formulate a fundamental unit to measure the testability of circuits, devices, subsystems, and systems. This formulation must be based on the foundations of reliability (Markov models), circuit sensitivity, controllability and observability, and other fundamental concepts which are involved in measuring the complexity, time, and effectiveness of testing.

2.0 Approach. This project involves a complicated analysis of many different disciplines and the program includes many different tasks.

2.1 Measure of testability. This task will involve the determination of a measure of testability based on review, analysis, and development involving several potential concepts for reaching a testability measure. Included are:

a. Sensitivity matrices. In all systems and circuits (analog or digital) it is possible to compute a sensitivity matrix which can be related to certain design parameters including a measure of testability. The sensitivity matrix must be investigated as a possible conceptual foundation that can become a basis of testability.

b. Controllability/observability based on optimal control. This task will address a measure of testability based on optimal control concepts including the controllability, observability, and identifiability principles. This conceptual investigation would utilize existing, proved engineering foundations and extend them to the problem of measuring testability.

c. Integrated measures of testability. This task will address the task of developing a procedure for giving a system a figure-of-merit for testability. This figure-of-merit should be formulated so that the contribution of each subsystem is easily identified and compared to the other subsystems. This will identify which subsystems have the most impact on overall system testability.

3.0 Scope. This task will have impact on the fault tolerance of the system under consideration. For this reason, the results of this study should be in a form that can be useful in determining the fault tolerance of a system.

4.0 References. See standard texts for the definitions of controllability and observability.

5.0 Background. A fundamental quantifiable parameter that is a measure of testability of the system would allow a hierarchical structure to be developed. Such a structure could identify the areas requiring more extensive testing, the points on partitions at which verification could be difficult. It is critical to the entire design and acquisition process that a quantification of testability be developed.

FAILURE-FAULT PREDICTION TECHNOLOGY

1.0 Introduction (objective). The purpose of this project is the development of the techniques, concepts, and methodology for failure-fault predictions. This project will encompass both analog and digital fault prediction. It will also address the system approaches necessary to exploit the capability of prediction.

2.0 Approach. A wide range of tasks is required in various areas.

2.1 Identification and classification of prediction capabilities. This task will determine which application circuits and systems can benefit from a failure and fault prediction capability. Emphasis will be on high-frequency analog circuits and systems, particularly in sensors and other high-power equipment.

2.2 Prediction algorithms for analog circuits. The task must develop a set of prediction algorithms and a theoretic foundation for their application in achieving fault prediction capabilities. It will involve the use of inherent circuit models and structures, as well as heuristic algorithms to evolve into practical prediction algorithms.

2.3 Feasibility of fault prediction in digital circuits. This task will determine the feasible approaches to fault prediction in digital circuits.

3.0 Scope. This project will explore the feasibility of fault prediction and will require a research approach that is based on all the foundations of test technology. This project must include demonstration systems to show feasibility.

4.0 References

- Fault Analysis in Affine Sequential Circuits, Seaks, R, Proceedings of the 1976 Conference on Information Sciences and Systems, p 227-232, Johns Hopkins University, March 1976 (with S Sangari)
- An Experimentation in Fault Prediction II, Seaks, R, Proceedings of the IEEE AUTOTESTCON, November 1977, Arlington, Texas, p 53 (abstract only)
- Fault Prediction Towards a Mathematical Theory, Seaks, R, Rational Fault Analysis, New York, Marcel Dekker, Inc (with L Tung and SR Liberty, to appear)
- A Functional Approach to Fault Analysis, Saeks, R, Rational Fault Analysis, New York, Marcel Dekker, Inc (with MN Ransom, to appear)
- Fault Tolerant Computing An Overview, Avizienis, A, IEEE Computer, vol 4, p 5-8, January-February 1971

5.0 Background. The advance of microelectronic technology will permit the monitoring and analysis of circuit and system parameters for fault and failure prediction. This capability will allow tremendous savings in maintenance and retrofit costs and significantly improve the fault tolerance performance of systems.

RECOVERY TECHNIQUES

1.0 Introduction (objective). It is the purpose of this project to develop approaches for effective application of recovery techniques to fault-tolerant systems. The fault-tolerant system concepts should be identified and the philosophies, protocol, and implementation problems associated with fault recovery should be addressed. In addition, costs, tools, and techniques for fault tolerance recovery approaches should be identified.

2.0 Approach. This project will involve various levels (hierarchy) of recovery techniques from the component and device levels through the system level.

2.1 Component and device voting techniques. This task will consider the technical issues and technology involved in voting and other component fault recovery techniques.

2.2 Functional fault recovery. Often faults can be detected in functional form and recovery is made to compensate for this functional failure. Functional faults are detected at the system level, although recovery can be accomplished at the functional level, subsystem level, and system level and either in hardware or software or both. This task will develop the technology required for designing fault recovery techniques including specifications, techniques, and tools.

2.3 Software recovery techniques. Software recovery algorithms are used to reconfigure at the subsystem and system level. This task will analyze and develop the theory of system recovery techniques using software. It will determine their performance and cost-effectiveness, implementation problems, and design tools.

3.0 Scope. This project is considered as a separate technical area and can be treated that way. However, it is recognized that it will be dependent upon several other projects in the theory of testing. It will be influenced by and directly affect other design criteria and design procedures.

4.0 References

- The Design of Totally Self-Checking Combinational Circuits, Smith, JE, Report 4-737, thesis, August 1976, University of Illinois, Urbana, IL
- On the Existence of Combinational Networks with Arbitrary Multiple Redundancies, Smith, JE, Metze, G, Report R-692, October 1975, University of Illinois, Urbana, IL

5.0 Background. Recovery techniques in fault-tolerant systems are implemented to compensate for detected faults and these techniques are germane to the successful design of systems. In their simplest form they consist of voter circuits; in the more complex systems they consist of extensive and complicated software programs. The theory of fault recovery is generally considered a system engineering decision process. This project will develop the system design approaches for effective application of recovery techniques.

TRANSIENT FAULTS

1.0 Introduction (objective). The goal of this project is to develop a methodology for use in systems design to make systems fault-tolerant to transient faults. The transient faults may be very short, ie, the drop of a bit in a data stream, or longer burst errors in which there is a series of faults in a contiguous group. The methodology should address both detection and correction of transient faults.

2.0 Technical approach. The following tasks are critical to this project.

2.1 Definition and classification. This task will provide the foundation for the research into transient faults. It will define the different classes of transients in terms of speed, nature of occurrence, and impact. The physical nature of transient faults will be considered and related to the testing problems that each poses.

2.2 On-line built-in-test for transients. The advance of component and device technology has pointed to the feasibility of monitoring circuits in an on-line continuous test that can detect transient faults. Once they are detected, recovery can be applied. This task will analyze, review, and develop techniques for on-line circuit testing and concurrently assess the cost-effectiveness of this approach.

2.3 Software recovery for transients. Transients require recovery techniques identical to methods used for permanent faults. This task will assess the effectiveness and practicality of software recovery techniques as applied to transient faults.

3.0 Scope. This project will be treated separately from other testing research because of its unique character. This project is one that involves investigating the underlying physical phenomena as well as testing techniques.

4.0 References

- The STAR (Self-Testing and Repair) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design, Avizienis, A, Gilley, GC, et al, IEEE Transactions on Computers, vol C-20, no 11, p 1312-1321, November 1971

5.0 Background. Transient faults occurring in electronic systems are difficult to cope with due to their elusive nature. Techniques are needed to detect and isolate them. This project will address the nature of transient faults and the test techniques which are applicable. Transients are serious if they are not part of a self-compensating system (eg, using roll-back or built-in-test). They introduce errors randomly and usually when least desirable; therefore, they can be catastrophic. In the past such faults were accepted as undetectable as well as impossible to isolate; however, recent advances in technology indicate that they can be determined and corrected. In addition, once detected, they can be used to predict overall failure of the device/system.

IDENTIFICATION OF FAILURE MODES

1.0 Introduction (objective). The goal of this project is to identify and classify failure modes that are likely to occur in the various classes of systems.

2.0 Approaches. The potential failure modes for different types of circuits will be identified and categorized. The following types of equipment should be considered:

Analog modules

Digital modules

Combination analog and digital modules

Shipboard equipments

Airborne equipments

Shore-based equipments

Other types that may have unique features or characteristics

To gather data on failure modes for these equipments, at least the following sources of information should be used: Navy repair depot records, Navy shipboard repair records, and Navy shore station repair records.

After the basic data are gathered, they should be grouped by type of failure, frequency of failure, cost of repair, and other categories.

3.0 Scope. The scope of this project takes in all types of military electronic equipment, at all maintenance levels.

4.0 References

- Design Validation in Hierarchical Systems, Losleban, P, 12th Design Automations Conference, p 431-438, 23-25 June 1975, Publ IEEE, National Security Agency, MD
- A Highly Efficient Redundancy Scheme Self-Purging Redundancy, Losq, J, IEEE Transactions on Computers, vol C-25, no 6, p 569-578, June 1976, Stanford University

5.0 Background. Fault-tolerant design that is based on statistical failure rates is one of the basic requirements for a realistic design and requires realistic failure rate data. These data have to be organized into categories by type of equipment. Failure mode data can then be used to establish guidelines for fault-tolerant design.

FAULT-TOLERANT SOFTWARE

1.0 Introduction (objective). It is the purpose of this project to develop a theoretical foundation for detecting and isolating errors in software. It must also address the recovery concepts that can be applied. This program should relate the theoretical foundation to problems of system verification, fault tolerance, and other specific software design efforts.

2.0 Approach. This program will consist of the following sequence of tasks.

2.1 Techniques of software testing. This task will review, analyze, and develop techniques for testing and analyzing software to determine the extent to which it performs the logical functions intended by its creator.

2.2 Theory of software testing. This task will determine the extent to which a theory of software testing is feasible and will develop the areas required to complete the theory.

2.3 Program verification. The need to verify correctness and provide for fault tolerance is related to the mathematical proofs that demonstrate the logical behavior of a program is as specified. It is also related to the constructive approach, which stresses correct development of a program. Both of these approaches rely on the programmer's ability to abstract properties of the program. These are referred to as inductive proofs of correctness.

3.0 Scope. This project must be addressed from the perspective of the software engineer who is concerned with the correctness and robustness (fault tolerance) of software. It should result in guideline standards and a set of recommendations for specifying, verifying, and design of software.

4.0 References

- Toward a Theory of Test Data Selection, Goodenough, JB, and Gerhart, SL, PROC ACM 1975 International Conference on Reliable Software, ACM, New York 1975, p 493-570
- ACM Computing Surveys: Special Issue on Reliable Software I: Software Validation, vol 8, no 3, September 1976
- Probabilistic Models for Software Reliability Prediction, Martin L Shoomar, Assoc Prof of EE, Poly Tech, Brooklyn, 1972 International Symposium on Fault-Tolerant Computing, Newton, MA, June 19-21, 1972
- F-T Software for Real-Time Applications, H Hect, AERO Space Corp, El Segundo, CA, ACM Computing Surveys, Special Issue, Reliable Software II: Fault-Tolerant Software, vol 8, no 4, December 1976, p 391-407
- Design of Self-Checking Software, SS YAU and RC Cheung, IEEE Proceedings of 1975 International Conference on Reliable Software
- System Structure for Software Fault Tolerance, Randell, B, Sigplan Not, vol 10, no 6, p 437-439, June 1975, University of Newcastle Upon Tyre, England
- Software Design Validation Tool, Carpenter, LD, Tripp, LL, Sigplan Not, vol 10, no 6, p 395-400, June 1975, Boeing Computer Services, Inc, Seattle, WA

- Fault-Tolerant Software for Spacecraft Applications, Hecht, H, Final Report, 10 December 1975, Aerospace Corporation, El Segundo, CA, contract F04701-75-C-0076

5.0 Background. Reliable software implies robustness (fault tolerance). That is, it is expected to deliver a certain minimum level of services even when faced with an unexpected or hostile environment (such as hardware failure or bad data). Techniques for detection and isolation of faults are classified into testing (analysis of responses of a selected set of input data) and verification (mathematical proof and constructive approach).

HIGH-ORDER LANGUAGE CONSTRUCTS FOR FAULT-TOLERANT SYSTEMS

1.0 Introduction (objective). The purpose of this project is the analysis and development of fault-tolerant language constructs suited for inclusion in the DoD high-order language standard.

This project will address language constructs that allow incorporation of program redundancy into a block-structured program in a well structured manner. It will not address system architecture and design methodologies for fault-tolerant programs.

2.0 Approach. The project will be conducted in the following sequence of tasks.

2.1 Analyze fault-tolerant program constructs. This task will collect, review, and analyze all constructs required for fault-tolerant programs. It will provide a list that can be incorporated in the DoD high-order language.

2.2 RMS-2 fault-tolerant constructs. The list of constructs will be reviewed for possible incorporation in the Navy's CMS-2 tactical language.

2.3 DoD high-order fault-tolerant constructs. The list of fault-tolerant program constructs will be reviewed for possible incorporation in extensible DoD high-order language standards. It will determine guidelines and recommendations for full use of fault-tolerant programs.

3.0 Scope. This project must be considered in relation to other research relative to fault-tolerant programs; namely, systems architecture and systems design methodology. However, this work can be performed concurrently with other efforts.

4.0 References

- Recent Developments in Software Fault-Tolerance Through Program Redundancy, Kim, KH, and Ramamoorthy, CC, Proc of the 10th Hawaii International Conference on System Science, January 6-7, 1977, p 234-239

5.0 Background. The most effective methods of meeting complex availability requirements and reducing development and support costs are to develop methodologies and tools for systematic incorporation of redundancy programming in a well structured form. Good structuring of a fault-tolerant program is particularly important, since the use of program redundancy increases the program size. Fault-tolerant programs have generally higher development costs and higher processing cost. The high processing cost of fault-tolerant programs is due to increased processor time and increased storage space required for executing redundant program components.

ANALOG FUNCTIONAL REDUNDANCY

1.0 Introduction (objective). This project will address several approaches that will result in the use of functional redundancy in analog circuits. This project must achieve a structuring of analog fault tolerance test techniques and capabilities. It must identify those characteristics of analog circuits which can be exploited in systems. It must demonstrate, through examples, the capabilities that are possible by quantitative analysis and test evaluation. Analog circuits span the entire known frequency range, are both high and lower power, and represent a complexity of functions that rivals the ability of digital circuits.

2.0 Approach. This project will consist of several concurrent tasks, with each contributing to the overall understanding and development of analog functional redundancy techniques. These are as follows.

2.1 Classification of analog functions. The wide range of analog circuits and functions will be classified into structures that can be a basis for applying various redundancy concepts. These classifications may be frequency, power, size, and other characteristics. The task should be conducted from the perspective of the designer who must use fault tolerance to achieve design objectives.

2.2 Redundant sensors. Analog sensors have been a continuous source of failures. Techniques should be analyzed, developed, and documented to permit more reliable sensing systems. Included in this task are phased array antennas and sonar transducers as well as other pressure, temperature, and environmental sensors.

2.3 Redundant filters techniques. Among the most commonly used analog functions is signal filtering. The task will address the use of redundancy in filter arrays. This problem is particularly critical in radar, EW, and sonar signal processing applications.

2.4 Analog control reliability. The control (analog or digital) of analog circuits is critical to complex array processing, and this task will address the area of redundant and built-in test in control. Such a task will be critical to redundant/voter circuit design. It will address the apparent vs the real need for a highly reliable voter circuit.

3.0 Scope. This project must draw upon existing and planned systems design, for example, and future analog functions. This project must involve experts in signal processing, systems engineering, and component and device technology.

4.0 References

- Research on Fault Analysis of Analog Circuits, Bedrosian, SD, Ho, DeYuan, interim report, Office of Naval Research, Alexandria, VA, August 1976, contract N00014-75-C-0768, University of Pennsylvania

5.0 Background. Analog circuits provide a unique challenge to fault-tolerant design since they are particularly complex and far more prone to failure than digital circuits. Analog circuits often require close component tolerances that tend to slowly degrade. This slow degradation presents a special challenge to the designer of redundant circuits.

FUNCTIONAL TEST DESIGN THEORY

1.0 Introduction (objective). Functional test is an area in which little theory of testing has been developed. This project will develop the theory of functional testing, from its theoretical foundations to its principles of application in systems, software, and hardware. This program can become the basis of functional testing of microcomputers as well as analog functional testing.

2.0 Approach. The project involves the following sequence of tasks.

2.1 Theory of functional test. The basic mathematical engineering foundation of functional test should be developed in a manner similar to that of software module definition. This task should address definition in terms of completeness and consistency. These concepts should produce an approach toward performing functional tests that are related to technology, although, in some isolated cases, the approach may be independent of technology.

2.2 Analogy functional test. Concepts for analog functional test should be evaluated, analyzed, developed, and documented. This task should be an extension of the above task.

2.3 Digital (microcomputer) functional test. The technique to functionally test a microcomputer or equivalent digital logic is the primary objective of this task. Based on task 2.1 above, this task should demonstrate and prove the applicability of functional test to microcomputers.

3.0 Scope. This project should be related to the next higher (and lower) level of the test hierarchy. This relationship is critical to the successful development of a fault-tolerant systems capability.

4.0 References

- A Graph Model for Fault-Tolerant Computing Systems, Hayes, JP, IEEE Trans Comput, vol C-25, no 9, September 1976
- A Reliability Model for Various Switch Designs in Hybrid Redundancy, Ingle, A, Siewiorek, DP, IEEE Transaction Computers, vol C-25, no 2, pp 115–133, February 1976, Carnegie-Mellon University

5.0 Background. Functional testing has often been left out of a system design until the last stages. This leads to testing as an add-on, rather than a built-in, function. If a good applied theory of testing is developed, functional testing can become part of system design from the beginning. In addition, functional testing can become the control portion of a fault-tolerant system design.

FAULT TOLERANCE VALIDATION AND VERIFICATION

1.0 Introduction (objective). The purpose of this project is the development of a sound approach for the validation and verification of fault tolerance systems capability. This project will address the validation and verification problem from the perspective of the systems acquisition manager, beginning with operational requirements and proceeding through systems acceptance test and evaluation. This project must identify techniques, tools, and standards that will simplify the verification process and improve its effectiveness. It must consider all concepts within the context of coping with the increasing complexity of advanced systems due to new component and device technology.

2.0 Approach. There are several important concepts that can be integrated into a sound approach to validation and verification. Each concept addresses different steps in the design and acquisition process and can be combined into an integrated approach.

2.1 Verification of specifications/standards. The operational requirements must be translated into specifications so that the requirement can be traced into the specification. In addition, specifications that guarantee that a requirement is satisfied must be identified. The analysis tools that permit verification of specifications must be identified and, if necessary, developed. It is possible that the risk, reliability, and systems analysis tools for system concept formulation are similar, if not identical, to the tools necessary for validation and verification.

2.2 System concept formulation – verification and validation. The formulation of system concepts is critical to life-cycle costs. In particular, system concept will affect about 70% of the life-cycle costs, and it is necessary to select the best concept in terms of cost. This task will determine the first stages of system concept formulation techniques.

2.3 Design for validation and verification. Design of a system should provide a structure that can lead to simplification of the validation and verification process. Functional and mechanical partitioning must be performed to permit testing of various components and functions independently; then an approach must be provided for verification of integrated systems. This task will address fault-tolerant design rules that will lead to design of verifiable systems.

2.4 System acceptance test theory. This task will develop the theory of performing system acceptance test and evaluation.

3.0 Scope. The perspective of the verification task is one which addresses the constructive techniques and further recognizes that many other areas/projects have immediate and direct relationship to verification. The project must be conducted by personnel with a combination of skill and experience in various disciplines.

4.0 References

- An Artwork Design Verification System, Baird, HS, Cho, YE, 12th Design Automations Conf, p 414–420, 23–25 June 1975, RCA Laboratories

5.0 Background. Without verification procedures it will be difficult, if not impossible, for the government to put a fault tolerance requirement into a system specification. There must be a clearly defined procedure for the government to use in buying a system from a contractor; otherwise the fault-tolerant specifications can only be design goals and not design requirements.

ESTIMATION OF CONFIDENCE LIMITS TESTING LARGE LOGIC NETWORKS

1.0 Introduction (objective). The purpose of this project is to provide a methodology and means for accurately determining confidence limits for the reliability of large digital logic networks without exhaustively exercising all possible input sequences or simulating all logical faults in the network. This will involve development, implementation, and demonstration of a logic simulation and fault analysis system that will serve as a tool for determination of reliability confidence limits of digital networks consisting of up to 15 000 elements by simulating selected combinations of faults against specific sequences of operations and, from the absence of these faults, inferring the correctness of the entire system.

Faults will be modeled via probabilistic techniques, and will occur singly and in multiple. The system, when completed, should be capable of reasonably approximating the actual operation of an existing logic network, including occurrence and location of failures, when all necessary processing and operating parameters are input to the model.

2.0 Approach. This project will be accomplished in a series of several interrelated tasks.

2.1 Simulation model. This task will include devising a simulation model for large logic blocks that is economical in terms of host computer storage and speed of simulation yet is sufficiently adaptable that a number of different, simultaneous failure mechanisms can be accommodated.

2.2 Failure injection routines. This task will create a set of probabilistic failure injection routines for use with the simulator developed in 2.1 above. The routines will be based on logic operation and observed anomalies.

2.3 Combining failure routines with simulator. This task will consist of combining the simulation and the failure injection routines developed in 2.2 above, then adjusting them to correctly predict the operation of logic modules with simple (one or two parameters) defect mechanisms.

2.4 Confidence limits. This task will include both (a) relating confidence limits to non-exhaustive measures of correctness of logic operation, and (b) devising methods of measuring the thoroughness of tests and assigning confidence limits to these.

2.5 Small-scale demonstration. This task will combine tasks 2.1 through 2.4 into a small-scale demonstration on a general-purpose computer and extend these techniques for larger logic blocks and more simultaneous defect mechanisms.

2.6 Techniques for larger logic blocks. This task will extend the above tasks into larger logic blocks and more simultaneous defect mechanisms. Included in this task is the conceptual design of a system to perform prediction of confidence limits for up to 15 000-gate networks, including data base and processing requirements.

2.7 Validation. This task will validate the system through comparison with actual tests of well characterized, known defective logic networks, and then a demonstration of a small-scale digital network on the system will be performed.

3.0 Scope. This project will involve logic designers that have worked with a number of different circuit card testers.

4.0 References

- Reliability Modeling of NMR Networks, Abraham, JA, Siewiorek, DP, June 1974, avail NTIS, Springfield, VA
- A Logic System for Fault Test Generator, Akers, SB, Jr, IEEE Transactions on Computers, vol C-25, no 6, p 620-630, June 1976, GE Electronics Laboratory, Syracuse, NY

5.0 Background. A number of logic card testers have been built that may be adapted to testing fault-tolerant digital cards. How the various systems can be adapted and used will be of great importance for maintaining digital equipment.

COMMAND CONTROL FAULT TOLERANCE

1.0 Introduction (objective). The goal of this project is to develop a design and evaluation methodology for fault-tolerant command control global networks. The methodology should address transient faults, permanent faults, and spoofing faults in relation to the system as an entity and in relation to each of its major components ADP systems, communication systems (inter- and intra-platform), sensor systems, weapons systems, and human systems.

2.0 Approach. The project should first address each class of faults separately, then address the problem of the design and evaluation of systems that encompass all the classes of faults. Specifically, the tasks are to identify and then investigate the impact on command control system components and the total system of

Transient faults - both long term and short term,

Permanent faults - single and multiple,

Spoofing faults -- detection and countermeasures, and

Combinations of the above classes of faults

and then to develop a methodology to evaluate fault-tolerant C^3 systems.

The particular parameters which need to be addressed in relation to the different classes of faults are

Survivability

Responsiveness

Availability

Flexibility

Invulnerability

Interoperability

Usability

Capacity

3.0 Scope. This project will be concerned with improving the performance of the military's command control and communications systems (C^3). An overall understanding of the C^3 will be needed by personnel assigned to this project.

4.0 References

- Navy Command Control and Communication System -- System Concept, Naval Warfare Effectiveness Group, NOSC, San Diego, California, 12 July 1976
- Navy Command Control and Communications System Definition of Performance Measures, Naval Warfare Effectiveness Group, NOSC, San Diego, California, 1 January 1977

5.0 Background. The availability of the military C^3 systems on a global basis is of major importance, especially during the periods preceding and during a conflict. A fault-tolerant design could contribute to the availability of a system during critical periods.

Because of the many sensors now available, the sophisticated data processing, and man-machine interfaces required, it is critical that fast communications be available within a platform, among platforms, and on a global basis to give a commander critical information when he needs it. This is true during the entire conflict scale from a prehostilities crisis to global war because data acquired from local sensors as well as from those operated by shore-based commanders in support of task forces will be correlated and evaluated in near real time as inputs to a commander's decision-making process. Timeliness and accuracy are paramount to this process.

Because of the long range of modern weapons a small conflict can have worldwide impact. Therefore, it is important that a local commander have highly reliable and flexible communications with higher authorities and also, in the other direction, communications with those under him. A missile fired by mistake, or at the wrong target, could be a disaster.

ARCHITECTURES FOR AVAILABILITY REQUIREMENTS

1.0 Introduction (objective). The purpose of this project is the review, analysis, and development of system architecture and networks which will result in increased fault-tolerant systems capabilities. Through this project, system architecture tradeoffs will be established and applied, to determine practical system structures meeting all requirements. This project must address the selection of architectures with regard to many different criteria, including cost, timing (queuing), complexity, maintainability, and automatic recovery.

2.0 Approach. This project will have the following tasks.

2.1 Analysis of classical architectures. This task will evaluate existing distributed architectures such as the STAR and the RING, and other classical multiprocessor configurations will be analyzed for their ability to operate in a fault-tolerant condition. This task will provide detailed analysis, simulation, or other data that will permit quantification of the results.

2.2 Distributed nets of computers. This task will result in the formulation of an approach to permit quantitative evaluation of networks. Current techniques have not addressed this issue, and extensive development of the foundations of fault-tolerant evaluation is necessary. This task combines the use of reliability models with queuing models (or other performance analysis tools).

2.3 Signal processing and analog system architectures. The analog and signal processing architectures requiring extensive design in fault tolerance capabilities will be investigated by this project. Distributed sensors such as phased array antennas, transducers, and banks of filters will be reviewed for fault tolerance design capabilities. A detailed analysis will be provided.

3.0 Scope. This project must be coordinated with other important research areas including microcomputers, fault prediction, and the taxonomy of fault tolerance and maintainability.

4.0 References

- Theory of Fault Tolerance 1976 Annual Report, vol I and II, contract N00014-75-C-0011, Office of Naval Research, December 7, 1976
- Fault-Tolerant Computing: An Introduction, Avizienis, A, National Science Foundation, Grant no MSC 72-03633 A4, Computer Science Dept, UCLA, Los Angeles, CA 90024, January 22, 1977

5.0 Background. Current efforts select structures which are intended to meet performance bounds and only later is it discovered that the fault tolerance requirements cannot be met.

The importance of this project is reflected in the fact that system architectures for meeting performance designs are in conflict with those for fault-tolerant design (eg, performance design dictates single centralized processing, while fault tolerance design requires distributed processing and multichannel communications).

COMMUNICATION PROTOCOL FOR FAULT TOLERANCE

1.0 Introduction (objective). Bus protocol for the reconfigurability of bus structured system architecture is critical to simple and cost-effective system design. This project addresses the various requirements and specifications that lead to standardization of bus protocol. It will include, to a lesser extent, the feasibility of technology-independent input-output (I/O) interfaces. The bus protocol will establish which units are master and slaves, which unit will transmit and/or receive. It will address the set of commands and acknowledgments that are necessary to determine which unit has failed, where the unit is, and what recovery procedures are to be taken. This project is critical to future distributed fault-tolerant systems design.

2.0 Approach. This project will review, analyze, and catalog the characteristics of various existing and proposed bus protocols and interface techniques to determine their applicability to fault-tolerant system design. It will ultimately provide recommendations for selection of these techniques as military standards.

3.0 Scope. The project must be conducted to achieve simple design of distributed computer systems. It is a project that will be critical to exploiting microcomputers in large networks. The project must be conducted in a way to maximize the military's use of new technology without introducing additional life-cycle costs in the support of nonstandard interfaces.

4.0 References

- MIL-STD-1553
- SDMS
- ANSI

5.0 Background. The area of bus protocol – I/O interface has been one of continued concern, as evidenced by the references.

SECTION A4.

SPECIFICATION PROJECTS

SPECIFICATION FOR REDUNDANCY MANAGEMENT

1.0 Introduction (objective). It is the purpose of this project to develop a common approach to fault tolerance system design through redundancy management. It will encompass the exchange of information within industry and the R&D community and develop state-of-the-art requirements for redundancy management.

2.0 Approach. The goal of this project is to develop a common approach to redundancy methods for system design. The project will consist of the following tasks.

2.1 Analyze fault-tolerant redundancy design techniques. Collect, review, and analyze various fault-tolerant system design techniques used in government and industry today.

2.2 Develop redundancy management techniques. Assemble the data developed in 2.1 above into redundancy techniques for use by system designers as a guide in developing a common approach to system design.

3.0 Scope. This project must be considered in relation to other research relative to fault-tolerant programs; namely, systems architecture and systems design methodology. This project can be performed concurrently to the other efforts.

4.0 References

- Fault-Tolerant Computing: An Introduction, Avizienis, A, UCLA, Los Angeles, January 22, 1977. Work supported by NSF Grant no MCS 72-03633 A04
- Computer Redundancy: Design, Performance, and Future, RE Kuehn, IEE Transactions on Reliability, vol R-18, no 1, February 1969, p 3-11

5.0 Background. Industry is currently developing and using systems that exploit the theory of redundancy. Although redundancy is used in many areas to develop more "reliable" systems, its use is usually an individual decision. The general lack of technical sources and a common exchange of knowledge in the application of redundancy for system design, construction, and testing of fault-tolerant systems clearly indicates a need for development of specifications and standards addressing redundancy management.

STANDARDS AND FAULT TOLERANCE

1.0 Introduction (objective). The goal of this project is to make recommendations for modifying existing military specifications to include fault-tolerant design. The specifications to be addressed are the Standard Electronic Module (SEM), DoD-1 high-order languages, built-in-test circuits, built-in-test design handbook, MIL-STD-1329 (Test Points and Interface Selection), and others.

2.0 Approach. This project is directed toward functions and control of standardization through the following tasks.

2.1 Definitions. This task reviews and updates all definitions, terminology, and other symbols that reflect the requirements, specification, and test of fault-tolerant systems. It will consolidate definitions, for both military and other organizations, into a useful form for use by the military.

2.2 Standard specifications. As fault tolerance technology matures, a set of standard specifications will be evolved and then applied. This task will lay the groundwork for this standard to be developed and applied.

2.3 Standards – software and hardware. Standard Electronic (AVIONICS) Modules (SEMs) and Standard Software Modules (SSMs) are fundamental to the simplification of design and maintenance and are critical to the reduction of life-cycle costs. This task will review current and proposed efforts and will indicate developments which will foster the advance of fault-tolerant technology.

2.4 Test and evaluation. Fault tolerance acceptance testing is important to the life-cycle cost and performance effectiveness of military systems; this task will address the practicality of standards in testing.

2.5 Other standards. Operational requirements through evaluation can benefit from the use of standards. This task will explore the practicality of their use in the design and acquisition cycle.

3.0 Scope. This project will require interaction with all other tasks to determine the characteristics and effectiveness of standards. This project should be performed in-house to obtain insight into methods for applying standards.

4.0 References

- Standardization, Verman, Lal C, Archor Books, 1973

5.0 Background. The use of standards is necessary for simplified, cost-effective application of fault tolerance in military systems. Among the standards to be reviewed, developed, and improved, relative to fault tolerance, are Standard Electronic Modules (SEMs), Requirements/Specification Standards, DoD-1 higher-order language, built-in-test circuits, built-in-test design handbooks, and MIL-STD-1329 (Test points and Interface Selection). This task will be instrumental in obtaining fault-tolerant capability in all military systems.

SECTION A5.
DESIGN PROJECTS

SELF-DIAGNOSING DESIGN TECHNIQUES

1.0 Introduction (objective). This project will study and analyze architecture, functional partitioning, and module and component design features necessary for achieving self-diagnostic microprogrammable capabilities in processors. The project will result in a set of guidelines for designing LSI components and modules that ensure testability of the component and the system employing the component. Redundancy levels, organization of functions, requirements for test points to be made accessible, and procedures for using these data to design and implement a self-diagnosable processor to the replaceable module level will be postulated and verified. The project will result in definition of general specifications for design and utilization of LSI components and modules in self-diagnosing systems.

2.0 Approach. Several tasks are required in a variety of areas.

2.1 Definition of baseline processing requirements. A set of processing requirements will be selected as a baseline for the comparative design of the self-diagnostic processors. Because the thrust of this project is demonstration of the self-diagnostic properties, an extensive set of baseline requirements is not necessary. However, requirements must be sufficient to validate the demonstration with respect to airborne processors rather than with respect to a trivial set of requirements.

2.2 Comparison of competing approaches. A comparison of self-diagnostic design techniques applied to both processors constructed of bit-slice components and processors constructed of monolithic components will be made to determine the proper level of partitioning for self-diagnosability. While it may be premature to estimate production costs of the processors, those characteristics that are known to contribute to cost will be examined. The comparison will consider the following characteristics at a minimum:

Simplicity of design

Parts count (variety of parts)

Component count

Availability of components

Performance

Programmability

Reliability

Testability

The evaluation will result in a top-level design of a processor having the desired self-diagnostic capabilities and meeting the baseline requirements for each of the competing approaches. At the end of this task the competing designs and results of the evaluation will be reviewed and a selection made of the approach to be pursued during the remainder of the project.

2.3 Processor design. The design approach selected in 2.2 above will be extended, during this task, to include:

Selection of components

Layout of processor

Specification of components

Generation of logic diagrams

Selection of instruction set

Writing of microcode

Simulation of processor

Evaluation of self-checking coverage

Identification of risk areas requiring verification

A design review will be held at the conclusion to evaluate the design. The high-risk areas, to be further refined, will be selected at this design review.

2.4 Processor simulation. The self-diagnosing processor will be simulated in order to demonstrate that the design will perform as required and to resolve conflicts and uncertainties in the design. Development of a detailed instruction level simulation is not intended as part of this task, but a top-level event simulation capable of identifying conflicts and races at the register level will be required. Some detailed simulation of portions of the processor may also be required.

2.5 Breadboarding of high-risk circuits. Implementation of a self-diagnosing processor may require unproved circuits and circuit technologies. In an attempt to reduce the risk associated with these circuits, breadboarding may be desired. Those devices and circuits that are estimated to be of high risk will be identified in 2.2 above and presented during the design review.

3.0 Scope. This project will explore the feasibility of developing a cost-effective and practical approach to designing a self-diagnosing fault-tolerant computer. This will be accomplished through the study, analysis, and simulation of techniques and components that can be used in digital systems that are self-diagnosable to the replaceable module level, resulting in a set of design specifications for module design that ensures self-diagnosability.

4.0 References

- US Air Force, Air Force Systems Command, Aeronautical Systems Division/PPM EA Wright-Patterson AFB, Ohio 45433, Solicitation F 33615-77-R-1106, 25 August 1976
- Synthesis and Analysis of a Cost Effective, Ultra-Reliable, High Speed, Semiconductor Memory System, EW Husband and SA Szygenda, IEEE Transactions on Reliability, vol R-25, no 3, August 1976, p 217–223
- System Fault Diagnosis Masking, Exposure and Diagnosability Without Repair, Russel, JD, IEEE Transaction Computer, vol C-24, no 12, p 1145–1155, December 1975, University of Wisconsin
- Managing the Development of Reliable Software, Williams, RD, Sigplan Not, vol 10, no 6, p 3–8, June 1975, TRW, Redondo Beach, CA
- Reliable Hardware Software Architecture, Wulf, WA, Sigplan Not, vol 10, no 6, p 122–130, June 1975, Carnegie-Mellon University, Pittsburgh, PA

- Design of Self-Checking Software, Yau, SS, Cheung, RC, Sigplan Not, vol 10, no 6, p 450–457, June 1975, Northwestern University, Evanston

5.0 Background. Most large computers have dedicated processors that continually test the health of the main processors. This philosophy may possibly be used with LSI components. If an LSI component could signal its own failure, that signal could become a control signal in a fault-tolerant system.

REDUNDANT MICROCOMPUTERS

1.0 Introduction (objective). The purpose of this project is the review, analysis, and development of redundant microcomputer concepts for fault-tolerant systems design.

2.0 Approach. It is necessary to formulate a baseline that will be a structure for the analysis and design of redundant computers. It will be achieved through the execution of several concurrent tasks.

2.1 Redundant computer analysis. The previous use of redundancy with general-purpose computers has been successfully applied, and this task will analyze advantages, disadvantages, major design characteristics, etc, of the configurations. The analysis must address the major characteristics that are applicable to use with microcomputers.

2.2 Memory sharing redundant configurations. Many applications require shared programs that are stored in a memory common to many processors. This task will analyze and develop redundancy concepts involving memory interleaving, switching input/output, and hardware executives/voters. This task should implement the most unique concept and then evaluate the results.

2.3 No-voter redundant microcomputers. Through a series of bus data interchanges, a set of microcomputers can detect and isolate failed microcomputers in the configuration. This task will analyze and develop protocol, data checking, and control procedures that allow microcomputer redundant configurations without voting circuits. The analysis must address reliability in quad-redundant configurations and compare no-voter designs against designs which employ conventional voting circuits.

2.4 Dedicated redundant microcomputers. Microcomputers will be employed in dedicated configurations, in which dedicated implies that the microcomputers implement an algorithm that remains unchanged throughout the life of a system. This task will explore the use of redundant microcomputers in achieving fault tolerance for dedicated computer configurations. It will also consider bus structures, interfacing, detection techniques, and other design considerations in developing a sound design methodology.

2.5 Redundant microcomputer methodology. The previous tasks will be assembled into a structured design baseline for future system design using redundant computers. It must represent a complete description of the design methodology from operational requirements to specifications, design, and system acceptance test.

3.0 Scope. This is a highly specialized and critical project because the microcomputer is constantly introducing new design concepts. Each of the tasks must be addressed in a manner that results in new innovative concepts.

4.0 References

- The STAR (Self Testing and Repairing) Computer: An Investigation of the Theory and Practice of Fault Tolerant Computer Design, A Avizienis, GC Gilley, FP Mathus, DA Rennels, JA Rohr, and DK Rubin, IEEE Transactions on Computers, vol C-20, no 11, November 1971, p 1312-1321

5.0 Background. The advent of the one-chip microcomputer has opened possibilities of new approaches for redundant computer configuration that exploit hardware executives, simplified voting circuits, and reduced switch complexities. Use of redundant microcomputers is now considered cost-effective and feasible for broad classes of problems. This project will formalize the approaches to applying redundant computers from analysis, design, and verification.

LOOSELY COUPLED FAULT-TOLERANT COMPUTER NETWORKS

1.0 Introduction (objective). The objective of this project is to develop a theory that will address problems of loosely coupled computer networks. Loosely coupled computers are those between any two of which there is only one-way communication. This implies that the receiving machine must always be ready to receive data (otherwise the data will be lost) and be able to error detect and/or correct data.

2.0 Approach. By use of directed graph theory, procedures will be developed to calculate the fault tolerance of a loosely coupled computer network.

3.0 Scope. This project will use graph theory coding and computer design specialists.

4.0 References

5.0 Background. Often a system – for example, a command control system – has long distances between its various subsystems. Because of the long distances, the communication paths have large delays in them. If a message is not received correctly, it is impractical to immediately notify the sender and retransmit the message. Also, there is no immediate feedback to the sender for verifying the message was sent correctly. This constraint on a system presents problems that may change system design in order to make it fault-tolerant.

FAULT TOLERANCE MASKING HAZARDS

1.0 Introduction (objective). The purpose of this project is to analyze and develop techniques for addressing fault tolerance systems design and use of redundancy. The goal of this project will be to investigate contemporary problems associated with redundancy, in particular those associated with masking (or static redundancy), and develop a set of design guidelines to help system designers avoid problems in designing, using static redundancy.

2.0 Approach. This project will consist of the following tasks:

a. Develop a listing of design features for system designs that use static redundancy to achieve fault tolerance.

b. Using the list of design features as a reference, develop a set of design goals for a fault-tolerant system that will use static redundancy.

c. From the design goals, prepare a document that gives the design information for meeting design goals.

3.0 Scope. The scope of this project is to take the theory given in the references and then adapt it to information that can be used by a system designer. The personnel performing this project require both theoretical and practical systems design backgrounds.

4.0 References

- Fault-Tolerant Computing: An Introduction, A Avizienis, UCLA, Los Angeles, January 22, 1977. Work supported by NSF Grant no MCS 72-03633 A04
- The Attainment of Reliable Digital Systems Through the Use of Redundancy – A Survey, RA Short, IEEE Computer Group News, vol 2, no 2, p 2-17, March 1968
- Mathematical Theory of Reliability, RW Barlow and F Proschan, New York, Wiley and Sons, 1965
- Probabilistic Logics and Synthesis of Reliable Organisms from Unreliable Components, J Von Neuman, CE Shannon, and J McCarthy, ed, Annuals of Math Studies No 34, Princeton University Press, 1956, p 43-98
- Real Time Fault Detection for Small Computers, JR Allen and SS Yau, AFIPS Conference Proc, vol 40, 1972

5.0 Background. In a fault susceptible system, fault tolerance can be implemented through the use of protective redundancy that will functionally take action when a specified fault occurs.

One method of fault tolerance redundancy that has been employed is fault-masking by using redundancy in such a fashion that the fault will be completely contained within a system module. As long as the built-in redundancy has not been exhausted, no symptoms will appear outside the module. However, when the redundancy has been exhausted or overwhelmed by a fault module, failure will result. Separate detection and recovery functions are not identified from outside the module. Thus, masking is often called a static redundancy technique.

The use of static hardware redundancy is based on the assumption that failures in the redundant copies are independent. For this reason the use of static redundancy is difficult

to justify within integrated circuit packages, due to the likelihood of failures affecting several adjacent circuits or components.

The forms of static redundancy that have been applied to space program computers have been the application of replication of individual electronic components and Triple Modular Redundancy (TMR) with voting. Several other applications have been studied, but never implemented because of the excessive cost of special components that were beyond the state of the art.

Some disadvantages of fault masking redundancy are:

a. Excessive costs associated with massive replication (three, four, or more times the basic system elements).

b. The requirement that assumes independent failures of the replicas.

c. The absence of warning when a module exhausts its redundancy and finally will fail.

Fault masking is similar to fault avoidance. While it may postpone the time of failure, the module will still fail suddenly and irrevocably when its redundancy is exhausted.

Regardless of the disadvantages, masking is a popular approach because of conceptual simplicity, instant reaction to a fault, and the fact that it is entirely transparent to the user. In particular, a promising area of application is protecting a "hard core" for which other approaches are prohibitively costly.

FAULT TOLERANCE DESIGN HANDBOOK

1.0 Introduction (objective). The summation of technological data on fault tolerance technology should be contained in a fault tolerance design handbook, and this task will develop the handbook to assume the widespread dissemination of data.

2.0 Approach. This program is a continuous collection and assessment of technology maintained by the military for use by industry in system design.

3.0 Scope. This project is conducted to achieve a handbook useful to both the system engineer and designer.

4.0 References

- The Design of Totally Self-Checking Systems, David Su Ming Ho, Coordinated Science Laboratory, Report R723, April 1976, UILU-ENG76-2211, University of Illinois
- General Design Rules for the Construction of m-out-of-n Totally Self-Checking Checkers, James E Smith and Gernot Metze, Coordinated Science Laboratory Report R-693, University of Illinois UIL – ENG – 75-2228, October 1975

5.0 Background

DESIGN/DEVELOPMENT TOOLS (METHODOLOGY)

1.0 Introduction (objective). Design and development of complex fault-tolerant systems involve many procedures, techniques, and methods that can be automated. In particular, tools can be automated for generation of tests, documentation, circuit simulation, and other functions. This project will address the development of the design and development methodology and the tools required to support it.

2.0 Approach. Many automated design and development tools will be included in this project. The key task is the development of an overall design and development methodology. This task must be performed in consonance with other tasks outside the area of fault tolerance technology.

3.0 Scope. This is a project which should naturally be included within the realm of design automation and methodology.

4.0 References

5.0 Background. Presently there are no methods (or tools) available to the system designer for developing fault tolerance system design. There is a need to assemble procedures, techniques, and methods to assist the system designer.

SECTION A6.

TEST AND EVALUATION PROJECTS

ACCEPTANCE TESTING

1.0 Introduction (objective). The goal of this project is to develop acceptance testing procedures for fault-tolerant systems. These procedures need to address testing for transient faults, permanent faults, and masked faults.

2.0 Approach. The following tasks are to be accomplished for this project.

2.1 Review of standards. Review existing military standards on acceptance testing and list those tests that may change when applied to testing a fault-tolerant system.

2.2 Document changes. Write recommended changes to the military standards including the rationale for making the changes.

3.0 Scope. This project will be involved with all types of acceptance testing and contract conditions.

4.0 References

- MIL-STD-781D, Reliability Tests Exponential Distribution, 15 November 1967
- Project Engineering, Hajek, VG, McGraw-Hill Book Co, New York, 1965

5.0 Background. Fault-tolerant systems continue to operate normally even though there has been an internal failure. Therefore, the normal methods of testing will not detect this type of failure; however, the system is still degraded. For example, when one of two redundant paths has failed, the next failure will shut down the system. Because of this, it will take special testing procedures to meet the fault-tolerant specifications.

TECHEVAL – OPEVAL TECHNIQUES

1.0 Introduction (objective). The technical and operational evaluation of fault-tolerant capabilities is critical to the development of new systems. Yet, the test and evaluation is difficult to accomplish after system design. The purpose of this project is (a) to assess the effectiveness of T&E after-design, and (b) to indicate techniques to perform more effective fault tolerance systems test and evaluation.

2.0 Approach. In concert with recognized test and evaluation agencies, this task will provide an assessment of techniques for fault tolerance test and evaluation. It will recommend new techniques for improvement of test and evaluation for fault-tolerant systems.

3.0 Scope. This project should be concerned with the additional complexity of systems that results from fault tolerance design.

4.0 References

5.0 Background

APPENDIX B:

FAULT-TOLERANT SYSTEMS
STATE-OF-THE-ART SUMMARY

SECTION B1. CURRENT RESEARCH

Title	Highly Reliable Civil Aircraft Computer Technology
Responsible organization	NASA, Aeronautics and Space Technical Office, Langley Research Center
Performing organization	NASA, Langley Research Center, Hampton, VA
Contract/grant	505-07-3:7670104 505-07-31:7570105 501-23-31:7470028
Principal investigator	Stitt, JE, Graves, GB
Period of performance	7/75 to 6/76; 7/74-6/75; 7/73-6/74
Objective	Initiate the logic design of two advanced fault-tolerant computer architectural concepts
Approach	Formal proofs of design will be developed to prove correct fault recovery strategies. Procedures for obtaining data inputs for reliability assessment tools will be developed, and reliability assessments will be performed for the fault-tolerant computer system designs. Software faults and their impact on systems reliability will be investigated. In-house investigations of off-the-shelf computer systems will be performed to gather data for determining that reliability improvements and fault tolerance are reliable.

Title	Distributed Computing for Real-Time Information Processing
Responsible organization	Naval Air Systems Command, Air 360, Comm, Control and Guidance, Washington, DC
Responsible individual	Zempolich, BA
Performing organization	NELC, San Diego, CA
Contract/grant	In-house
Principal investigator	Wong, HF
Period of performance	5/76-9/78
Objective	Quantify the All Applications Digital Computer (AADC) parameters required for a low-cost, fault-tolerant, real-time tactical system.
Approach	Based on work performed for the office of Naval Research by UCLA and NELC on distributed functions architecture and other related recent work, develop a distributed architecture model for a real-time tactical system such as NAVSEA's Surface Offensive Warfare Command Control System. Exercise the model and determine the parameters for processor partitioning, module interconnection, and intersystem interfaces.

Title	Adaptive Engagement Logic and Control Studies
Responsible organization	DA BMD Advanced Technology Center, ATTN: ATC-C, PO Box 1500, Huntsville, AL
Responsible individual	Smith, TO
Performing organization	TRW, Inc., TRW Systems Group, One Space Park, Redondo Beach, CA Systems Control, Inc, 1801 Page Mill Rd, Palo Alto, CA
Contract/grant	DASG60-76-C-0084
Principal investigator	Spadaro, FG (TRW) Spain, DS (Sys Contr, Inc)
Period of performance	4/76-11/75
Objective	The objective of this program was to formulate and develop advanced resource allocation and control techniques which will produce orders of magnitude of defense performance improvement. These advanced techniques should provide a wide range of optimal defense response to a broad spectrum of innovative offensive strategies and must consider projected technology advances in associated disciplines, such as sensors and interceptors. This effort extends the state of the art in BMD.
Approach	The approach that was used to accomplish the program objectives included: (1) conducting a requirements analysis study and defining resource allocation and control algorithm design requirements for both ground-based and missileborne applications; (2) conducting a survey of advanced information processing techniques to include pattern recognition, fault-tolerant logic, artificial intelligence, etc; (3) performing an adaptive engagement logic and control algorithm design study; and (4) producing a simulation (test bed) design that contains design features sufficient to demonstrate the validity of the approach for accomplishing the objectives of the program.
Progress	Information processing techniques with potential applicability to BMD control problems were identified, and examples of their use in a BMD context were provided. Results are documented in the final report entitled Adaptive Engagement Logic and Control Studies dated November 1975.

Title	Fault-Tolerant Computing
Responsible organization	US National Science Foundation, Division of Mathematics and Computer Sciences
Performing organization	University of California, School of Engineering and Applied Sciences, Computer Sciences, Los Angeles, CA
Contract/grant	MC572-03633, A00 through A04
Principal investigators	Avizienis, AA; Chu, WW; Martin, DF
Period of performance	Fourth Year 2/76-1/76 Fifth and final year 3/76-4/77
Objective	A 5-year continuing research effort focused on fault tolerance of computer systems.
Approach	This project is a continuing research effort focused on fault tolerance of computer systems. A fault-tolerant computer executes its entire set of programs correctly in the presence of faults in the computer system. Faults which occur in a computer system fall into two major categories: hardware faults, which include all deviations from design-specified values of logic variables within the hardware of the computer; and software faults, which include all deviations from correct program execution due to errors occurring during the translation of the original specification of an algorithm to the program being executed. The primary topics for study during the fourth year were Methodology of Fault Tolerance, Design and Modeling of Fault-Tolerant Systems, Multiaccess Memories and Distributed Data Base Systems, Program Correctness, and Software Reliability and Certification. The primary topics for study during the fifth and final year of the grant included Methodology of Fault-Tolerance, Design and Modeling of Fault-Tolerant Computer Systems, and Software Reliability.

Title	Organization and Technology -- Oriented Codes for Arithmetic and Memory Systems
Responsible organization	US National Science Foundation, Division of Engineering
Performing organization	Southern Methodist University, School of Engineering, Electrical Engineering, Dallas, TX
Contract/grant	ENG76-11237
Principal investigator	Rao, TR
Period of performance	5/76-/77
Objective	Investigate codes and coding techniques for fourth-generation computer arithmetic and memory systems.
Approach	The study is directed towards investigating codes and coding techniques for fourth-generation computer arithmetic and memory systems. Specifically, the techniques are to be technology-oriented and organization-oriented for the purpose of fault tolerance, improved performance, and reliability of operation. In addition, coding techniques which improve the yield of LSI memory chips and thus lower the cost per chip by a significant factor are studied. An important and challenging problem posed here is to determine the best (from the cost-performance point of view) approaches for "highly survivable memory" organizations and "byte-organized arithmetic processors." The most significant gain to be expected from coding is that with a given level of semiconductor technology, it will be possible to produce coded memory arrays of much larger size than would be economically feasible in the uncoded case.

Title	Information Management System
Responsible organization	NASA, Manned Space Flight Office, Marshall Space Flight Center, Huntsville, AL
Performing organization	NASA, Marshall Space Flight Center, Huntsville, AL
Contract/grant	910:7670706
Principal investigator	Panciera, RE
Period of performance	7/75-6/76
Objective	The objective of the Space Ultrareliable Modular Computer effort was to develop low-cost, reliable aerospace modular computers and computer input/output hardware which are applicable to NASA's future payloads.
Approach	The main thrust of this effort was to inject, into the current simplex design, adequate reliability by the incorporation of automated fault detection and correction designs; perform qualification testing; and continue to develop support software. The development of an internally fault-tolerant computer must be undertaken for timely integration of future payload information management subsystems such as the tug. The objective of the information management effort was to continue to define, develop, and space qualify an on-board Information Management System (IMS) which can best accomplish the requirements of the space tug missions. Areas in which analysis and technology developments are required will be identified. The requirements for memory will be determined. A computer previously developed under this effort and computer input/output hardware with special monitoring equipment currently under development will be provided for use in the design, development, and test of a redundant laser gyro inertial measuring unit.

Title	Symposium on Computer Software Engineering
Responsible organization	Air Force Office of Scientific Research, NE, Bolling AFB, Washington, DC
Responsible individual	Knausenberger, GE
Performing organization	Polytechnic Institute of New York, Brooklyn, NY
Contract/grant	AF-AF-SR-2891-75
Principal investigator	Oliner, AA
Period of performance	6/75-6/77
Objective	The twenty-fourth symposium of the Polytechnic Institute of New York scheduled for 20–22 April 1976 on the subject of Computer Software Engineering focuses attention on new fields of electronics research. Computer systems development depends significantly on improvements in planning, specification, design, acceptance, and deployment of software. Its relationships to computer operational reliability and availability must be defined, measured, and predicted. Related software research renders suitable probabilistic models; also, design techniques such as structured programming, team programming, and code reading promise more reliable initial designs. Broad fields of testing and analysis of programs and of computational operations and computer element utilization begin to emerge. The planned symposium will provide an international forum for the leaders in these areas to present their developing ideas, to interact, and (via the proceedings) to provide lasting documentation. The program being considered includes: in the area of reliability, topics such as program proofs and test models, reliability estimation and demonstration, operational reliability measurement, quality control measures, software maintenance models, and fault-tolerant software; in the area of software management, prerequisites and tools to aid program construction, configuration control, productivity, and planning and scheduling of programming; in the area of design, problems of measures of program complexity and information processing flow, of analysis of run time, calculation of memory size, and hardware/software trafeoff. The symposium is sponsored by the Air Force Office of Scientific Research, Army Research Office, and the Office of Naval Research under the Joint Services Electronics Program (JSEP) in cooperation with the Polytechnic Institute of NY. It has been assured of the

technical support of the IEEE Computer Society; also, the participation of the IEEE Group on Reliability and of the Association for Computing Machinery is being arranged.

Progress

30 June 75 – 30 June 76. The symposium on computer software engineering took place April 20 to 22 in New York with an attendance of about 250 professionals and with sessions on design techniques (three papers), requirements (five papers), models and data (six papers), theory (five papers), languages (four papers), reliability (seven papers), and case studies (five papers). Preparation of proceedings is in progress.

Title	Theory of Fault Tolerance
Responsible organization	Office of Naval Research, Arlington, VA
Responsible individual	Denicoff, MD
Performing organization	Honeywell, Inc, Systems Research Division, Minneapolis, MN
Contract/grant	N00014-75-C-0011
Principal investigator	Heimerdinger, WL
Period of performance	8/74-11/76
Objective	As more and more functions are given to computers, the need of the Navy for ultrareliable computers grows more acute. The general area of fault tolerance is of great importance. To date, no unified theory of fault tolerance exists that enables one to evaluate fault tolerance schemes, to make comparisons, or to determine design improvements for such devices. This work was aimed at the development of a systematic analytic framework to accomplish these important tasks.
Approach	Several graph modeling techniques have been identified as possible tools to use for this development. Specific tasks for this contract period are (1) to investigate the critical properties of data which must be incorporated into the graphical representation, in order to correctly model data contamination; (2) to clarify the distinction between data and control and formalize their interaction in the context of graphical techniques; and (3) to investigate the concept of hierarchy in labeled graphs.
Progress	Progress to date has shown a systematic and mechanizable technique for reducing a Petri net to a smaller Petri net, such that the smaller net preserves some properties of the original. The same systematic method can also verify that a Petri net possesses those desired properties. In order to reduce them systematically, it is necessary to identify some desirable properties of the nets and to determine mechanically whether a net possesses them. The desirable properties are primarily consistency and invariance and their relations with liveness, boundedness, and transition firing ratios. Refer to Heimerdinger, WL, and Jack, LA, A Graph Theoretic Approach to Fault-Tolerant Computing, 1975-76 Annual Report, 22 March 1976.

Title	Galois Logic for Fault Tolerance Detection in Computer Systems
Responsible organization	Office of Naval Research, Arlington, VA
Responsible individual	Denicoff, MD
Performing organization	Sperry Rand Corp, UNIVAC Defense Systems Division, St Paul, MN
Contract/grant	N00014-75-C-0675
Principal investigator	Marver, JM
Period of performance	7/74-6/76
Objective	There is a growing need in the Navy for more reliable computer systems. The general area of fault tolerance is of great importance in the effort to produce computing equipment with very high reliability. The mathematics of Galois logic is uniquely suited to systems which can be easily reconfigured to bypass certain components, thus tolerating faults in the system. This effort investigates Galois logic to apply its unique properties in the design of highly reliable computer hardware.
Approach	The contractor will investigate several configurations of Galois linear modules; several different error classes such as multiple bit errors in the same variable; and the feasibility of a particular method using Galois test polynomials for error detection, location, and suppression. The method, if feasible, will be generalized to larger arrays of Galois linear modules.
Progress	Fault detection and location algorithms have been developed for simple trees of Galois linear modules. They cover the 4-bit case and have been extended to the 8-bit and the 16-bit cases. However, much additional work remains to be done.

Title	Distributed Information Processing Systems Architecture
Responsible organization	Office of Naval Research, Arlington, VA
Responsible individual	Trimble, J
Performing organization	NELC, Communications Processing Division, San Diego, CA
Contract/grant	In-house
Principal investigator	Wong, HF (Code 3200)
Period of performance	10/74-9/79
Objective	Investigate the problem of control for a distributed information processing architecture, using minicomputers and microprocessors that can readily adapt to and recover from processor or bus/link failure.
Approach	Study distributed processing architecture. Study and analyze minicomputer and microprocessor interconnection techniques. Examine relevant data management and retrieval strategies. Analyze the asynchronous bus structure for processing element interconnection. Examine alternatives for an optimal distributed information system architecture relationship to the fault tolerance of the architecture.
Progress	A basic system bus structure has been described and allocation protocols have been defined for it.

Title	Command Control: Fault-Tolerant Input/Output Network
Responsible organization	Office of Naval Research, Arlington, VA
Responsible individual	Denicoff, MD
Performing organization	Charles Stark Draper Laboratory, Cambridge, MA
Contract/grant	N00014-76-C-0502 N00014-75-C-0500
Principal investigator	McKenna, JF
Period of performance	7/74-6/76; 3/76-2/77
Objective	The Navy has a need for highly reliable computer systems. The development of fault-tolerant theory and schemes for implementation is one important part in the development of ultrareliable systems. One key subsystem in any computer system is the input/output network. This task is directed toward the development of such a fault-tolerant subsystem.
Approach	A fault-tolerant network is being designed and fabricated to serve as the I/O network for a multiprocessor system. The I/O network is an alternative to I/O buses. Nodes of the network are used to route information. Configuration control is directed by a centralized processor. Control algorithms are implemented in software. This task involves evaluation of this network concept and development and evaluation of the necessary software. Such a network should provide both an economically viable alternative to a data bus and a significant improvement in reliability and survivability, particularly to physical damage.

Title	Distributed Processor/Memory Architectures
Responsible organization	Air Force Avionics Laboratory AAM, Wright-Patterson AFB, OH
Responsible individual	
Performing organization	Texas Instruments Inc, Dallas, TX
Contract/grant	DF096630:F33615-74-C-1018
Principal investigator	Consolver, G
Period of performance	7/74-6/75
Objective	Obtain detailed functional design from the distributed processor memory computer concept definition including fault-tolerant capability, modular expandability, and basic LSI compatible iterative structure.
Approach	Obtain executive control and application program base to support the system. Simulate the DP/M network at a functional level to verify the concept. Implement the flow chart design of the executive control program. Design an automated "Process Constructor" procedure for allocating applications programs to DP/M processors. Begin design of an HOL compiler compatible with the DP/M architecture.

Title	Command Control: Advanced Approaches to Computer System and Component Design
Responsible organization	Office of Naval Research, 430C, Arlington, VA
Responsible individual	
Performing organization	University of California, School of Engineering, Los Angeles, CA
Contract/grant	DN723247:N00014-69-A-0200-4027
Principal investigator	Ohu, W
Period of performance	7/74-6/75
Objectives	Continue research in the areas of computer architecture, fault-tolerant features of computer communications, and memory systems, as these subjects are important in Navy combat systems.
Approach	Demonstrate feasibility of new concepts with experimental hardware to make empirical measurements and to make comparisons with theoretically predicted results. In order to thoroughly test experimental devices, simulators have been built and monitor programs written.

Title	Adaptime Information Processing and Control Studies
Responsible organization	Department of the Army, Advanced Technology Center, Attn: ATC-C, Huntsville, AL
Responsible individual	Tubbs, L
Performing organization	Leland Stanford Jr University, c/o sponsored projects office, Stanford, CA
Contract/grant	OASG60-75-C-0095
Principal investigator	Widrow, B
Period of performance	6/75-11/76
Objective	Perform basic research in the information sciences and demonstrate how advanced information processing techniques might be applied to solving practical engineering problems encountered in developing real-time algorithms for advanced sensors and data processing systems. This effort will extend the state of the art in BMD.
Approach	The approach includes identifying and analyzing practical engineering problems encountered in developing real-time data processing techniques for information processing and control of advanced passive and active sensors. Consideration shall be given to sensor applications performing such functions as acquisition, track, object identification, and hand-over to other sensors. Information processing techniques to be considered will include artificial intelligence, pattern recognition, fault-tolerant logic, and other techniques that may be defined in the course of this study.
Progress	Progress includes defining the resource allocation problem in a game theoretic sense for both a terminal and area defense system configuration. Adaptive learning techniques are being applied to the solution of this problem and results will be compared to alternative solution techniques. Heuristic search and production rule concepts have been identified as candidates for detailed investigation.

Title	A Graph Theoretic Approach to Fault-Tolerant Computing
Responsible organization	Air Force Office of Scientific Research, Bolling AFB, Washington, DC
Responsible individual	Bram, Joseph
Performing organization	Honeywell, Inc, Minneapolis, MN
Contract/grant	F44620-75-C-0053
Principal investigator	Heimerdinger, W
Period of performance	2/75-1/77
Objective	Avionics systems are becoming the heart of almost all modern Air Force weapon systems. The growing central importance of the avionics system to overall system operation has highlighted the need for a systematic approach to avionics system design from a fault tolerance viewpoint. The objectives of this research program are to expand existing fault-tolerant digital systems and to develop a better representation of data in these systems. This research will contribute to the development of unified theory of fault tolerance for analysis and synthesis.
Approach	The influence of time on the functional behavior of digital systems and on fault detection and fault recovery in them will be investigated and a formulation developed to reflect this influence in the fault tolerance graph model. This would include determining when time is an important factor, documenting the assumption implicit in the incorporation of time in the model, developing the expanded model, and refining and evaluating the new model. In other work, the development of a representation for this data in fault-tolerant systems will be initiated.

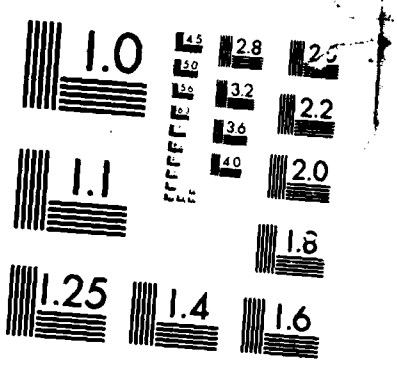
Title	Maintainability Prediction and Analysis
Responsible organization	Air Force, Rome Air Development Center RBR, Griffiss AFB, New York 13440
Performing organization	Hughes Aircraft Company, Fullerton, CA
Contract/grant	DF736770
Principal investigator	Pliska, T
Period of performance	7/75-6/76
Objective	Develop new maintainability prediction and analysis techniques based directly on the characteristics of equipment diagnostics and using built-in-reliability data and time standards.
Approach	Involved study and further development of the diagnostic, built-in, and external test equipment figures of merit such as those developed during this in-house phase of study. Definition of quantifiable means to evaluate or measure each such figure of merit, followed by the integration of such figures of merit with other directly quantifiable components of maintainability to form modeling and prediction relationships. In particular, the prediction technique involved relating each diagnostic routine (test circuit procedure, ie, automatic, semiautomatic, or manual) to the LRUs involved and determination of the proportion of faults possible in an LBU that will be detected by each diagnostic routine. Determining the proportion of failures expected from each LRU of an equipment. Defining the time required to isolate a failure to an LRU if a diagnostic (automatic) does not. Defining diagnostic ambiguities (diagnostic isolation to how many different LRUs) and the average time to isolate the faulted LRU under that circumstance. Time motion studies to define corrective action times. All these parameters are available from a design study of A/N equipment. This model will reflect three aspects of data handling: data access, data attributes, and data transformation.
Progress	1 February 75 31 January 76. The aim of this research is to develop a model, based on the theory of graphs, for the representation and analysis of fault-tolerant systems. Such a model could be of immense value in the design of future electronic hardware, and possibly in computer software. It was determined that the notion of Petri nets,

which are extensions of labeled graphs, would yield the most useful types of models for fault-tolerant systems. The fault phenomena commonly seen in digital systems were classified according to their observable effects, and it was found that six well defined functional fault classes were enough to encompass most of the faults that ever arise. Furthermore, the classification scheme can also be applied usefully to software. Some problems with the approach involve faults with data items, faults involving timing constraints, and faults moving in time into different classes. The efforts of the past year concentrated on control-related fault phenomena.

Title	Large Scale Computer Systems
Responsible organization	US National Science Foundation, Division of Mathematics and Computer Sciences
Performing organization	University of California, School of Engineering, Electrical Engineering and Computer Sciences, Berkeley, CA
Contract/grant	DCR72-03734-A01
Principal investigator	Ramamoorthy, CV
Period of performance	3/75-2/76; 3/76-2/77
Objective	Study large-scale computing systems with primary emphasis on pipeline processing.
Approach	Consideration will be given to parallel processing and the fault tolerance and reliability of these approaches. Included will be studies of the detection of parallelism in existing serial programs, schedule and utilization of parallel and pipeline resources, the detection of program characteristics (including parallelism) which have a marked effect on the utilization of a pipeline system organization, and parallel and pipelined fault diagnosis and recovery.

AD-A169 808 FAULT-TOLERANT SYSTEMS TECHNOLOGY PROGRAM PLAN: A CONCENTRATED PRIORITIZE..(U) NAVAL OCEAN SYSTEMS CENTER SAN DIEGO CA W J DEJKA 01 AUG 77 NOSC/TD-131 2/2

UNCLASSIFIED F/G 5/1 NL



MICROCOPY CHART

Title	Reliable Switching Circuits for Naval Communications
Responsible organization	Office of Naval Research, Arlington, VA
Responsible individual	Denicoff, M
Performing organization	Johns Hopkins University, Dept of Electrical Engineering, Baltimore, MD
Contract/grant	N00014-75-C-1196
Principal investigator	Masson, GM
Period of performance	6/75-9/76
Objective	Navy communications systems, both shipboard and shore-based, use very large switching networks. Presently, problems associated with these networks include high cost, individual switch characteristics, and network reliability. This task is aimed at studying the problems of reliability and its associated cost.
Approach	The contractor will perform research on the fault-tolerant aspects of large-scale switching networks. The continued development of general results and analytical tools will be stressed. The three areas of concentration for the study are: (1) fault detection, location, and recovery; (2) measures of fault tolerance within switching networks; and (3) development of simulation techniques for large-scale fault conditions.
Progress	While this effort has been underway only a short time, some progress has already been made. As the underlying basis of the interconnecting capability of binomial switching and linking systems, a theorem has been proved which specifies the formation of a family of subsets of a given set of elements for which any subset of this given set containing less than or equal to some fixed number of elements is a partial transversal.

Title	Design of Radiation-Hardened Digital Circuits and Systems
Responsible organization	AF Weapons Laboratory ELP, Kirtland AFB, Albuquerque, NM
Responsible individual	Simon, Robert G
Performing organization	University of New Mexico, Albuquerque, NM
Contract/grant	F29601-75-C-0041
Principal investigator	Devries, Ronald C
Objective	To analyze the effectiveness of two fault tolerance techniques and to develop other circuit hardening schemes for producing radiation-hardened large scale integrated (LSI) circuits for use in military applications.
Approach	The effort is divided into three phases. In the first phase UNM proposed techniques will be analyzed and compared with respect to effectiveness with other fault tolerance and error correction schemes. In the second phase, radiation-tolerant circuits will be designed via the most effective combination of these techniques. In the third phase, the circuits designed in the second phase will be analyzed by the contractor for electrical and radiation performance.
Progress	1 November 75 – 1 May 76. Data on distribution of failures due to radiation of assorted semiconductor devices are being assembled. The available data do not include as many devices as had been hoped, but will allow comparative failure analyses as intended. Flash X-ray tests of two sample circuits were completed and analysis of results is proceeding.

Title	Advanced Software Quality Assurance
Responsible organization	Army DA BMD, Advanced Technology Center, Kluntoville, AL
Responsible individual	Johnson, BA
Performing organization	General Research Corp, Santa Barbara, CA
Contract/grant	DASG60-76-C-0050
Principal investigator	Milton, R
Period of performance	3/76-5/77
Objective	Develop techniques that extend the state of the art in BMD by generating and proper insertion of assertions into a software package to support automated program correctness proofs.
Approach	Identify faults in support of fault-tolerant capabilities. They are developing techniques necessary to develop the assertions related to software reliability.

SECTION B2. ANNOTATED BIBLIOGRAPHY

Avizienis, A, Gilley, GC, et al, The STAR (Self-Testing and Repair) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design, IEEE Transactions on Computers, vol C-20, no 11, p 1312 - 1321, November 1971

Abstract

This paper reports the results obtained in initial studies which led to the design and construction of a computer with dynamic redundancy – called STAR. Several aspects of this computer (which went into operation in 1969) are discussed. Areas covered include architecture, reliability analysis, software, automatic maintenance of peripheral systems, and adaptation to serve as the central computer in an outerplanet exploration spacecraft. Techniques of fault tolerance went into the systematic design of STAR and were later applied to automatic maintenance of the Thermoelectric Outer Planet Spacecraft (TOPS).

Bedrosian, SD, Ho, DeYuan, Research on Fault Analysis of Analog Circuits, interim report, Office of Naval Research, Alexandria, VA, August 1976, contract N00014-75-C-0768, University of Pennsylvania

Abstract

Work involves development of inexpensive alternative approaches for fault analysis of analog circuits. The authors show a basis for the application of fuzzy set concepts and a new fuzzy fault dictionary approach. They want to apply adaptive learning techniques to augment fuzzy algorithms and make possible an "on line" procedure for fault isolation and location.

Chiang, ACG, Test Schemes for Microprocessor Chips, Computer Design, p. 87-92, April 1975

Abstract

Paper reviews modern microprocessor unit testing techniques in four considerations: computer simulation, signature testing, pattern recognition, and pattern generation. Advantages and disadvantages of the prevailing techniques are discussed with emphasis on the characterization-oriented techniques which fulfill most design needs. Author believes that end-users will adopt the techniques of pattern recognition and pattern generation because of their low cost.

Collins, EJ, Fairtest – A System for Computer Aided Design of Test Programs for Digital Logic Modules, Fairchild Systems Technology, Palo Alto, CA 94304, no date, etc

Abstract

Reports the development and use of the Fairtest computer aided test generation system tailored specifically for functional test pattern generation for digital logic modules. The paper describes the general nature and capability of the modules which make up the system, plus examples of application to a macro model of JK flip-flop and to a sample network which uses that macro.

Cottler, O, Testing of Complex Digital Multi-LSI Array Assemblies, RCA

Abstract

Appearance of high-complexity digital PCBs with 10 - 20 interconnected LSI chips and several MSI and SSI digital devices has caused the surfacing of a problem. That problem is the lack of proved cost-effective means to generate test programs for these boards.

RCA is looking at establishing test design criteria and surveying existing test design methods. Their approach is to consider testing very early in the generation of complex printed circuit boards.

Gates, JS, Electro-hydraulic Diagnostic Equipment, Chrysler Corp

Abstract

Reports on the development of new fault-isolation methods at the system level. The objective is to provide a low-cost Automated Universal Hydraulic Test Console configured for electro-hydraulic diagnostics and fault isolation. Work is a systematic approach to testing, validating, designing, and developing a hydraulic test console. Tradeoff studies were conducted to determine the effectiveness of a computer approach vs a semiautomated approach (switching logic) to test circuits.

Goodman, DM, Automatic Test Equipment for High Power Microwave Tubes and Systems, Davex Engineering Co, Report 100/3, San Diego

Abstract

The purpose of the task was to review the reliability and maintainability aspects of high-power microwave tubes and transmitters; to determine what sensors and data processors could be used to improve the automatic fault diagnostic capability in these tubes and transmitters; and to make plans for carrying out the recommendations resulting from the study. One of the recommendations was that the Navy initiate an R&D program titled ATE for High Power Signal and Control Electronics. The system reported upon was the AN/AWG-10 airborne fire control system utilized in the F-14 aircraft.

Hayes, JP, A Graph Model for Fault-Tolerant Computing Systems, IEEE Trans Comput, vol C-25, no 9, September 1976

Abstract

Paper presents a graph model (related to Hamiltonian graph theory) which explicitly represents computing systems and the algorithms to be executed. The graphs display the computing facilities involved in particular computations as well as the interconnections among them. The model allows for nonprobabilistic measures of fault tolerance according to Avizienis' definition of fault tolerance - "the ability to execute specified algorithms correctly, regardless of hardware failures and program errors." The model directly relates to the problem of determining minimum configurations or structure required to achieve a certain degree of fault tolerance.

Hayes, JP, On the Properties of Irredundant Logic Networks, IEEE Transactions on Computers, vol C-25, no 9, September 1976, USC

Abstract

This work investigated the constraints imposed on the structure of combinational logic networks by various types of irredundancy. These were classified as: (1) irredundancy, (2) redundancy, and (3) irredundancy which relates to certain types of network structures. The results presented have relevance to the problem of determining whether a given network contains redundancy.

Jack LA, Theory of Fault Tolerance, an Examination of a Design for Testability Methodology, vol II, 7 December 1976

Abstract

When compared to the significant costs of hardware procurement, the cost of system testing and support was considered to be secondary, but this emphasis has changed because of increasing system complexity. Design for testability has slanted towards a top-down methodological approach, which is what Jack talks about: "design more testable systems with minimal cost impact." The primary purpose of the paper was to outline the components of such a methodology.

Jack, LA, Heimerdinger, WL, Han, YW, Kinney, LL, Theory of Fault Tolerance, 1976 Annual Report, vol 1, 7 December 1976

Abstract

The authors explore labeled graph properties to successfully model fault-tolerant phenomena. A modeling hierarchy task demonstrated that Petri net structures could be reduced while preserving their intrinsic properties. Also investigated was a design for a testability methodology which was identified as a Navy-wide requirement. Another task was to formalize the interface between the data transformation structure and the control structure. This work indicated that a two-graph modeling approach was preferred over the single-graph approach.

Jack, LA, Heimerdinger, WL, Johnson, MD, Theory of Fault-Tolerance, 1974 - 1975 Annual Report, 22 September 1975

Abstract

This report details the efforts involved in representing fault-tolerant phenomena with labeled graphs. To provide greater flexibility over the STUCK-AT-ONE or STUCK-AT-ZERO models, two existing classical models were used to develop a theoretical base for design and evaluation of fault-tolerant digital systems. These existing labeled graphs are LOGOS and Petri nets. Results indicated that use of these models concisely described the intricacies of fault mechanisms.

Lovera, RAP, On Detection-Estimation Schemes for Signals with Uncertain Models, Report R-736, thesis, July 1976, University of Illinois, Urbana, IL

Abstract

Paper presents a new approach for estimating a random signal whose statistical description contains unknown parameters. The joint detection-estimation scheme consists of a bank of estimates and a detector to select the most appropriate estimator for each realization of the signal. This is illustrated by examples, and a general explicit solution for a continuous-time Gaussian is presented.

McCluskey, EJ, Wakerly, John F, Ogus, RC, Current Research, Technical Report 100, October 1975, Center for Reliable Computing, Stanford University

Abstract

This technical report summarizes the results of three projects related to computer reliability and fault tolerance. The first project concerns the theory of faults in logic systems and centers around the role of redundancy in the design of reliability models. This first project is very extensively annotated. The second study reported upon deals with the maintainability of computers, while the third project lends itself to the area of dual computer configurations as applied to guidance and navigation systems. The report lists many works in the field of computer reliability and fault tolerance.

Smith, JE, The Design of Totally Self-Checking Combinational Circuits, Report R-737, thesis, August 1976, University of Illinois, Urbana, IL

Abstract

Paper discusses the design of self-checking combinational circuits. Emphasis is given to the design of "totally self-checking check circuits," since a totally self-checking circuit is of little value if it itself cannot be checked. Fault models are discussed. Circuit designs which are totally self-checking with respect to unidirectional and single stuck-at faults are considered. Also, other sets of faults such as shorts, transients, and intermittent failures are discussed.

Smith, JE, Metze, G, On the Existence of Combinational Networks with Arbitrary Multiple Redundancies, Report R-692, October 1975, University of Illinois, Urbana, IL

Abstract

The report presents a few tools (math models, etc) for studying multiple-line redundancies for which any proper subset is irredundant. Also explored are several new examples of multiple redundancies, and it is proved by a constructive method that redundancies of all multiplicities exist. The authors state, however, that unintentional redundancy increases the costs of combinational logic networks and makes it difficult or impossible to diagnose all faults in the network.

Smith, JE, Metze, G, General Design Rules for the Construction of m-out-of-n Totally Self-Checking Checkers, Report R-693, October 1975, University of Illinois, Urbana, IL

Abstract

This report presents a set of conditions that characterize a class of realizations of m-out-of-n code totally self-checking checkers. A design method for minimal two-level checkers is given. A relationship between m and n is shown using a theorem from combinatories. Paper goes on to report the achievement of fault-tolerant systems through self-checking. Properties of totally self-checking checkers are given by defining circuits in terms of self-testing, fault-secure, totally self-checking, code disjoint, and totally self-checking checker.

Susskine, AK, Diagnostics for Logic Networks, IEEE Spectrum, p 40-47, October 1973

Abstract

Paper centers about the problem of testing large network arrays with a substantial lack of test points. An examination of functional and structural testing is made with most of the paper zoning in on structural testing techniques. Fault insertion vs fault simulation is discussed as is the difference between the popular D-algorithm and the Boolean-difference approach. The author favors the incorporation of diagnostics into design rules, and criticizes the development of diagnostics after the design has been completed.

NOTE: In the 3 years since this paper, the classical methods of test generation (D-algorithm and Boolean-difference) have been made useless by the doubtfulness of stuck-at models, complexity of chips, and unavailability of gate models for LSI units.

Yau, SS, Cheung, RC, Design of Self-Checking Software, Proceedings of 1975 International Conference on Reliable Software

Abstract

This particular paper gives visibility to different techniques for constructing a piece of self-checking software for systems requiring ultrareliability. Various self-checking capabilities (checks of functions, software errors, incorrect loop terminations, control sequence data for a process, illegal branches, etc) can be implemented during the initial stage of program development. The paper evaluates the cost-effectiveness of each technique in the particular operating environment.

SECTION B-3. GENERAL BIBLIOGRAPHY ON FAULT TOLERANCE

Abraham, JA, Siewiorek, DP, Reliability Modeling of NMR Networks, June 1974, avail NTIS, Springfield, VA

Akers, SB, Jr, A Logic System for Fault Test Generator, IEEE Transactions on Computers, vol C-25, no 6, p 620–630, June 1976, GE Electronics Laboratory, Syracuse, NY

Anon, International Conference on Reliable Software, vol 10, no 6, June 1975, 21–23 April 1975, IEEE, ACM, et al, Los Angeles, CA

Anon, A Module Interface Specification Language, 12 Design Automations Conference, p 42–49, 23–25 June 1975

Anon, International Symposium on Fault-Tolerant Computing, 4th Annual, Digest of Papers IEEE cat no 74, CHO864-9C, New York, NY 1974

Atanosov, Uy G, One Procedure for Designing S-Fault-Tolerant Discrete Devices, Avtom and Telemekh (USSR), vol 36, no 8, p 93–99, August 1975. Translation of, is in: Autom and Remote Control, vol 36, no 8, pt 1, p 1291–1296, August 1975

Avizienis, A, Approaches to Reliable Computing, Sigplan-not, vol 10, no 6, p 458–464, June 1975, UCLA

Baird, HS, Cho, YE, An Artwork Design Verification System, 12th Design Automations Conf, p 414–420, 23–25 June 1975, RCA Laboratories

Barsi, F, Maestrini, R, Grandoni, F, A Theory of Diagnosability of Digital Systems, IEEE Transactions on Computers, vol C-25, no 6, p 585–593, June 1976, Pisa, Italy

Batni, RP, Kime, CR, A Module-Level Testing Approach for Combinational Network, IEEE, Transactions on Computers, vol C-25, no 6, p 595–604, June 1976, University of Wisconsin, Madison

Blevins, PR, Read-Only Storage Failure Checking Technique, IBM Tech Disclosure Bull, vol 18, no 8, p 2402–2402, January 1976

Boehm, BW, McClean, RK, Urfrig, DB, Some Experience with Automated Aids to the Design of Large Scale Reliable Software, Sigplan Not, vol 10, no 6, p 105–113, June 1975, TRW, Redondo Beach, CA

Broen, RB, A Fault-Tolerant Estimator for Redundant Systems, IEEE Transaction Aerosp and Electron Sypt, vol AES-11, no 6, p 1281–1285, November 1975, McDonnell Aircraft Co

Brown, FM, Test Vector Generation for Internode and Input Diode Short Faults, 2nd USA Japan Computer Conference Proceeds, p 562–566, 1975, Published by AFIPS Honeywell

Bryan, RF, McAfee, JJ, Wells, PE, Danielson, WR, End-to-End Recovery, avail NTIS, Springfield, VA

Burstall, RM Darlington, J, Some Transformations for Developing Recursive Programs, Sigplan Not, vol 10, no 6, p 465–472, June 1975, University of Edinburgh, Scotland, Department of Artificial Intelligence

Cannon, WM, Chuang, HYH, Reliability Analysis of a Fault Restoration Scheme with Non-Perfect Restorer, Computer Science Conference, September 75 (abstracts only received) 54, 1975

Carpenter, LD, Tripp, LL, Software Design Validation Tool, Sigplan Not, vol 10, no 6, p 395-400, June 1975, Boeing Computer Services Inc, Seattle, WA

Carter, William C, McCarthy, Charles E, Implementation of an Experimental Fault-Tolerant Memory System, IEEE Transactions on Computers, vol C-25, no 6, p 557-568, June 1976

Case, GR, A Statistical Method for Test Sequence Evaluation, 12th Design Automations Conference, p 257-258, 23-25 June 1975, Sandia Laboratories, Albuquerque, NM

Chuang, HYH, Fail-Safe Asynchronous Machines with Multiple Input Changes, IEEE Transactions on Computers, vol C-25, no 6, p 585-593, June 1976, University of Pittsburgh

Cicu, A, Malocchi, M, Polillo, R, Sardoni, A, Organizing Tests During Software Evolution, Sigplan Not, vol 10, no 6, p 43-50, June 1975, Honeywell Info Sp, Italy

Courtois, B, Savcier, G, On Balancing Hardware – Firmware for Designing a Fault-Tolerant Computers' Series, Micro 8: Workshop on Microprograms, 8th Annual Proc, Chicago, IL, p 1-5, September 21-23, 1975, New York, NY 1975

Cox, GW, Carroll, BD, Reliability and Coverage Analysis of Nonrepairable Fault-Tolerant Memory Systems, final technical report, 1 July 1976, 106 p, Auburn University, AL, contract NAS8-26930

Crompton, JM, Proving of Software for Telecommunication Control, Intl Conf on Software Engr for Telecommunication Switching Systems, p 73-76, 18-20 February 1976, Plessey Telecom Ltd

Culpepper, LM, A System for Reliable Engineering Software, Sigplan Not, vol 10, no 6, p 186-192, June 1975, Naval Ship Res & Rev Center, Washington, DC

Das, SR, Bhattacharyya, A, A Novel Approach to Fault Detection and Design of Checking Sequences for Sequential Machines through Machine Modification by Augmentation of Special Inputs, Computer Science Conference, Sup 75 (abstracts only received), 54, 1975, 18-20 February 1975, ACM, University of Calcutta

David, R, Blanchet, G, About Random Fault Detection of Combinational Networks, IEEE Transactions on Computers, vol C-25, no 6, p 659-664, June 1976, Grenoble, France

Davis, AM, An Interactive Analysis System for Execution-Time Errors, University of Illinois

Degli, Antoni, G, Miglioli, P, Ornaghi, M, The Synthesis of Programs as an Approach to the Construction of Reliable Programs, p 327-352, 1975, 1-3 July 1975, European Assoc Theoretical Computer Science, Publ Inst Recherche D'Information and et D'Automatique, Univ di Milano

Dennis, NG, Thiss Voter – Switch Analysis, Proc Inst Electr Eng (GB), vol 120, no 9, p 954-958, September 1973

Dennis, NG, Probabilistic Reliability of a Canonical Fault-Tolerant Standby Redundancy, Proc Inst Electr Engr (GB), vol 123, no, 2, p 135-139, February 1976, GE Space Division

Durbro, EB, Design of a complete Fault-Detection Test for a Combinational Device from a Representative of its Equivalent Tree, Avtom and Telemkh, vol 36, no 1, p 154–161, January 1975, Trans of: Autom and Remote Control, vol 36, no 1, pt 2, p 139–145, January 1975

Edwards, NP, The Effect of Certain Modular Design Principles on Testability, Sigplan Not, vol 10, no 6, p 401–410, June 1975, IBM TJ Watson Res Con, NY

Fan, Yu-Dar, Design of Fail-Safe Asynchronous Sequential Machines, Technical Report, January 1976. Illinois University at Urbana-Champaign Coordinated Science Laboratory – Army Electronics Command, Fort Monmouth, NJ, contract DAAB07-72-C-0259

Fike, JL, Predicting Fault Detectability in Combinational Circuits – A New Design Tool? 12th Design Automations Conference, p 290–294, 23–25 June 1975, IEEE Southern Methodist University, Dallas

Fischler, MA, Firschein, O, Drew, DL, Distinct Software An Approach to Reliable Computing, 2nd USA Japan Computer Conference Proceedings, p 573–579, 26–28 August 1975, Lockheed, Palo Alto

Fridrich, M, Davis, WA, Further Results in Fault Detection for Combinational Circuits, Digital Processes (Switzerland), vol 1, no 1, p 25–37, Spring 1975, University of Alberta

Friedman, AD, Fault Detection in Redundant Circuits, IEEE Transactions on Electronic Computers, vol EC-16(1)

Gannon, JD, Horning, JJ, The Impact of Language Design on the Production of Reliable Software, Sigplan Not, vol 10, no 6, p 10–22, June 1975, University of Toronto, Toronto, Canada

Gilley, GC, Shared Memory for a Fault-Tolerant Computer, Patent, Patented on 13 April 1976, National Aeronautics and Space Administration Pasadena Office

Gilley, GC, A Fault-Tolerant Spacecraft, Digest of the 1972 International Symposium on Fault-Tolerant Computing, p 105–109, June 19–21, 1972

Halton, D, Implementation of a Fault Tolerant Computing System for Communication Control, Int Conf on Computer Communications (ICCC), 2nd, Proc, Stockholm, Sweden, August 12–14, 1974, p 555–559, Publ by Int Council of ICCC, Stockholm, Sweden, 1974, Plessey Telecommun Res, Dorset, England

Hayes, JP, Transition Count Testing of Combinational Logic Circuits, IEEE Transactions on Computers, vol C-25, no 6, p 613–620, June 1976

Hecht, H, Fault-Tolerant Software for Spacecraft Applications, Final Report, 10 December 1975, Aerospace Corp, El Segundo, CA, contract F04701-75-C-0076

Hemming, CW, Jr, Hemphill, JM, Digital Logic Simulation Models and Evolving Technology, 12th Design Automations Conference, p 85–91, 23–25 June 1975, IEEE, AGM

Ho, David Su-Min, The Design of Totally Self-Checking Systems, Technical Report, April 1976, Illinois University at Urbana-Champaign Coordinated Science Laboratory, contract DAAB07-72-C-0259

Hoare, CAR, Data Reliability, Sigplan Not, vol 10, no 6, p 528–533, June 1975, Queens University of Belfast, Ireland

Ingle, A, Siewiorek, DP, A Reliability Model for Various Switch Designs in Hybrid Redundancy, IEEE Transaction Computers, vol C-25, no 2, p 115–133, February 1976, Carnegie-Mellon University

Karavai, MF, An Algorithm of Construction of a Multi-Fault Detection Test for Combinatorial Circuits, Avtom and Telemekh (USSR), vol 36, no 1, p 162–170, January 1975, Trans of: Autom and Remote Control, vol 26, no 1, pt 2, p 146–153

Kohavi, Z, Berger, I, Fault Diagnosis in Combinational Tree Networks, IEEE Transaction Computers, vol C-24, no 12, p 1161–1167, December 1975, University of Utah

Losleben, P, Design Validation in Hierarchical Systems, 12th Design Automations Conference, p 431–438, 23–25 June 1975, Publ IEEE, National Security Agency, MD

Losq, J, A Highly Efficient Redundancy Scheme Self-Purging Redundancy, IEEE Transactions on Computers, vol C-25, no 6, p 569–578, June 1976, Stanford University

Lynch, WC, Langner, JW, Schwartz, MS, Reliability Experience with CHI/OS, Sigplan Not, vol 10, no 6, p 252–259, June 75, Case Western Reserve University, Cleveland, OH

Maheshwari, Shachindra N, Hakimi, S Louis, On Models for Diagnosable Systems and Probabilistic Fault Diagnosis, IEEE Transactions on Computers, vol C-25 no 3, p 228–236, March 1976, Grant AF-AFOSR-2103-71

Maheshwari, SN, Graph-Theoretic Models for Diagnosis of Digital Systems, Availability: Univ Microfilms, Ann Arbor, MI, order no 75-7950

Manning, FG, Automatic Test, Configuration, and Repair of Cellular Arrays, June 1975

Marver, JM, Fault Tolerance in Galois Trees An Algorithm for Detection and Location of Stuck-At Type Errors in Trees of Galois Linear Modules, June 1975

Mathur, FP, DeSousa, PT, Reliability Modeling and Analysis of General Modular Redundant Systems, IEEE Transaction Reliab, vol R-24, no 5, p 296–299, December 1975, University of Missouri

McCluskey, EJ, Ogus, RC, Survey of Computer Reliability Studies, Electro-Technol (India) vol 19, no 4, p 82–95, December 1975, Stanford University

Merlin, PM, A Study of the Recoverability of Computing Systems, Univ Microfilms, Ann Arbor, MI, no 75-11026, University of California, Irvine

Merlin, PM, Farber, DJ, Recoverability of Modular Systems, Proceedings of the ACM Sigcomm/Sigops Interprocess Communications Workshop, p 51–56, 24–25 March 1975, ACM, NY

Meyer, JF, The Reliable Design of Software A Formal View and a Survey, International Computer Symp, p 253–261, 2–4 June 1975, University of Michigan, Ann Arbor

Meyer, JF, Computation-Based Reliability Analysis, IEEE Transactions on Computers, vol C-25, no 6, p 578–584, June 1976, University of Michigan

Miller, EF, Melton, RA, Jr, Automated Generation of Testcase Datasets, Sigplan Not, vol 10, no 6, p 51-58, June 1975, Gen Res Corp, SB, CA

Mills, David L, Transient Fault Recovery in the Distributed Computer Network, interim report, February 1976, Maryland University, College Park Department of Computer Science

Neumann, George W, Automatic Testing, A Tool for Improving Fleet Readiness, a paper presented 12 March 1976 at the Annual Tech Symp Assoc of Science and Engineering of the Naval Air and Sea Systems Commands, Naval Material Command, Washington, DC

Newman, Bernard J, A Self-Repair Multifunction Design Analysis, report, July 1969, Army Electronics Command, Fort Monmouth, NJ, Communications/ADP Laboratories, project DA-1-H-062101-A-327

Palit, A, Chattopadhyay, DK, Basu, MS, Chaudhury, AK, Realization of Fault-Tolerant Machines, Computer Science Conference/Sup 1/75 (abstracts only), 54, 1975, 18-20 February 1975, ACM, University of Calcutta

Parnas, DL, The Influence of Software Structure on Reliability, Sigplan Not, vol 10, no. 6, p 358-362, June 1975, Tech Univ, Darmstadt, Germany

Postlethwaite, CW, Griswold, H, Mettler, GP, A Guide for Preparing and Evaluating Built-in Test Performance Specifications, Final Report, August 1970, Arinc Research Corporation, Annapolis, MD, contract N00019-69-C-0321

Ramamoorthy, CV, Vih, Wa Han, A Reliability Analysis of Systems with Concurrent Error Detection, IEEE Transaction Computers, vol C-24, no 9, p 868-878, September 1975, UCB

Ramamoorthy, CV, HO, SF, Testing Large Software with Automated Software Evaluation Systems, Sigplan Not, vol. 10, no 6, p 382-394, June 1975, UCB

Randell, B, System Structure for Software Fault Tolerance, Sigplan Not, vol 10, no 6, p 437-439, June 1975, University of Newcastle Upon Tyre, England

Rao, JR, Impact of Program Restructuring on Software Reliability, Computer Science Conference/Sup 1/75 (abstracts only received), 33, 1975, 18-20 February 1975, ACM, Washington, DC, State University of New York, Plattsburgh

Reifer, DJ, Automated Aids for Reliable Software, Sigplan Not, vol 10, no 6, p 131-142, June 1975, Aerospace Corp, El Segundo, CA

Russel, JD, System Fault Diagnosis - Masking, Exposure and Diagnosability without Repair, IEEE Transaction Computer, vol C-24, no 12, p 1145-1155, December 1975, University of Wisconsin

Schneidewind, NF, Analysis of Error Processes in Computer Software, Sigplan Not, vol 10, no 6, p 337-346, June 1975, Navy Postgraduate School, Monterey, CA

Scola, P, An Annotated Bibliography of Test and Diagnostics, Honeywell Computer Journal, vol 6, 1972

Shedletsky, JJ, McCluskey, EJ, The Error Latency of a Fault in a Sequential Digital Circuit, IEEE Transactions on Computer, vol C-25, no 6, p 655-659, June 1976, Stanford University

Sklaroff, JR, Redundance Management Technique for Space Shuttle Computers, IBM Res and Dev, vol 20, no 1, p 20-28, January 1976

Terplan, K, Measurements for Improving Reliability, Computer Science Conference/Sup 1/75 (AOR) 30, 1975, 18-20 February 1975, ACM, Washington, DC, USA, Hungary, Comp Centre, ASSN

Thompson, EW, Szygenda, SA, Three Levels of Accuracy for the Simulation of Different Fault Types in Digital Systems, 12th Design Automations Conference p 105-113, 23-25 June 1975, University of Texas, Austin, TX

Torin, JM, Fault Tolerant Computing in Satellites, J Br Interplanet Soc, vol 2a, no 4, p 219-231, April 1976, Saab-Scania, Goteborg, Sweden

Ultrasystems, Inc, Irvine, CA, Analysis of the Survivability of the Shuttle (ALT) Fault Tolerant Avionics System, Appendices, final report, April 76, contract NAS9-14739

Ultrasystems, Inc, Irvine, CA, Analysis of the Survivability of the Shuttle (ALT) Fault Tolerant Avionics System, final report, April 1976, contract NAS9-14739

Walczak, K, Decomposition Application to the Synthesis of Hazard Free Circuits for Adjacent Changes, Pr Inst Masz Mar (Poland), vol 17, no 3, p 35-53, 1975, Polish language

White, DW. Fault Detection through Parallel Processing in Boolean Algebra, March 75, avail in NTIS, Springfield, VA

Wilcox, JD, Retroactive Failure Correction for Strapdown Redundant Inertial Instruments, J Spacer and Rockets, vol 12, no 6, p 363-367, June 1975, TRW Sp Group

Wilcox, P, McCready, WJL, An Emulator for an Automatic Test System, 12th Design Automations Conference, p 286-289, 23-25 June 1975, IEEE, AGM Bell - Northern Res. Ottawa, Canada

Williams, RD, Managing the Development of Reliable Software, Sigplan Not, vol 10, no 6, p 3-8, June 1975, TRW, Redondo Beach, CA

Wulf, WA, Reliable Hardware - Software Architecture, Sigplan Not, vol 10, no 6, p 122-130, June 1975, Carnegie-Mellon University, Pittsburgh, PA

Yau, SS, Cheung, RC, Design of Self-Checking Software, Sigplan Not, vol 10, no 6, p 450-457, June 1975, Northwestern University, Evanston, IL

INITIAL DISTRIBUTION

AIR FORCE AVIONICS LABORATORY
WRIGHT-PATTERSON AFB, OH 45433
DR C BRODNAX (10)
MAJ BUSH

AIR FORCE ASD
WRIGHT-PATTERSON AFB, OH 45433
JOHN WEBER

ARMY RESEARCH OFFICE
BOX CM, DUKE STATION
DURHAM, NC 27702
DR WILLIAM SAUNDERS

NAVAL AIR SYSTEMS COMMAND
NAIR-360 (B ZEMPOLICH)

OFFICE OF NAVAL RESEARCH
ONR-437 (J TRIMBLE)

NAVAL ELECTRONIC SYSTEMS COMMAND
CODE 330 (R FRATILLA)
CODE 33013 (R KAHANE)
CODE 33015 (J MACHADO)
CODE 3041 (J CAUFFMAN)

NEW LONDON LABORATORY
NAVAL UNDERWATER SYSTEMS CENTER
NEW LONDON, CT 06320
CHUCK ARNOLD

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
77 MASSACHUSETTS AVE
CAMBRIDGE, MA 02139
DR LIBA SVOBODOVA
DAVE JENSEN

CARNEGIE-MELLON UNIVERSITY
PITTSBURGH, PA 15213
DR DAN SIEWIOREK

VIRGINIA POLYTECHNIC INSTITUTE AND
STATE UNIVERSITY
BLACKSBURG, VA 24061
DR FG GRAY, DEPT OF EE

UNIVERSITY OF CALIFORNIA
LOS ANGELES
LOS ANGELES, CA 90024
DR A A AVIZIENIS

STANFORD UNIVERSITY
STANFORD, CA 04306
DR EJ MC CLUSKEY, DIGITAL SYSTEMS
LABORATORY

STANFORD RESEARCH INSTITUTE
333 RAVENSWOOD AVE
MENLO PARK, CA 94025
MR JACK GOLDBERG

HONEYWELL SYSTEMS AND RESEARCH CENTER
2600 RIDGEWAY RD
MINNEAPOLIS, MN 55413
MR LARRY JACK

TRW
1 SPACE PARK
REDONDO BEACH, CA 90278
MR CAY WEITZMAN

TEXAS INSTRUMENTS
PO BOX 6015, MS #269
DALLAS, TX 75222
MR BUDDY DEAN

CHARLES S DRAPER LABORATORY
68 ALBANY STREET
CAMBRIDGE, MA 02139
AL HOPKINS

DAVEX ENGINEERING
SAN DIEGO, CA
C/O CODE 921
NAVAL OCEAN SYSTEMS CENTER
SAN DIEGO, CA 92152
DR DAVE GOODMAN

DEFENSE DOCUMENTATION CENTER (12)

END

DTIC

7-86